REPUBLIKA E SHQIPËRISË

KONTROLLI I LARTË I SHTETIT

DEPARTAMENTI I AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT

RAPORT AUDITIMI PERFORMANCE

"Siguria kibernetike në infrastrukturën kritike E-Taxation"

TIRANË 2025

P Ë R M B A J T J A

PËRMBLEDHJA 4
1. PROBLEMI SOCIAL DHE RËNDËSIA E AUDITIMIT 5
1.1 Konteksti i problemit social 5
1.2 Rëndësia e auditimit të performancës 6
1.3 Auditime të mëparshme apo aktuale në këtë fushë 6
2. SUBJEKTET NËN AUDITIM 7
2.1 Hyrje në subjektet nën auditim 7
2.2 Baza ligjore që rregullon çështjen nën auditim 11
Kriteret politike: 11
2.3 Rëndësia e produkteve të subjektit 12
2.4 Pesha në buxhet 14
2.5 Përkufizimet dhe terminologjia 14
2.6 Skema e analizës së programit auditues 16
2.7 Feedback-u i subjektit në fazën studimore 17
3. DETAJET E AUDITIMIT 17
3.1 Vlerësimi i risqeve të aktiviteteve të subjektit 17
3.2 Objektivi i auditimit 18
3.3 Pyetjet e auditimit 19
3.4 Fushëveprimi i auditimit 19
4. SHTJELLIMI I PYETJEVE AUDITUESE 20
4.1 A është korniza rregullatore aktuale e mjaftueshme për mbrojtjen kibernetike? 20
4.2 A janë ndërmarrë masa organizative, për parandalimin, mbrojtjen ndaj cenimeve kibernetike? 25
4.3 A janë ndërmarrë masa teknike, për parandalimin, mbrojtjen dhe reagimin për sigurinë kibernetike? 29

AKRONIMET

RSH	-	Republika e Shqipërisë
BE	-	Bashkimi Evropian
KLSH	-	Kontrolli i Lartë i Shtetit
AKSK	-	Autoriteti Kombëtar për Sigurinë Kibernetike
AKSHI	-	Agjencia Kombëtare e Shoqërisë së Informacionit
DPT	-	Drejtoria e Përgjithshme e Tatimeve
SEI	-	Software Engineering Institute
ISO	-	International Organization for Standardization
OIKI	-	Operatorë të Infrastrukturave Kritike të Informacionit
OIRI	-	Operatorë të Infrastrukturave të Rëndësishme të Informacionit
DRC	-	Disaster Recovery Center
DRP	-	Disaster Recovery Plan
BCC	-	Bussines Continuity Center
BCP	-	Bussines Continuity Plan
INTOSAI	-	The International Organization of Supreme Audit Institutions
EUROSAI	-	The European Organisation of Supreme Audit Institutions
ENISA	-	European Union Agency for Cybersecurity

PËRMBLEDHJA

Auditimi me temë “Siguria kibernetike në infrastrukturën kritike e-Taxation” ka pasur si objektiv kryesor vlerësimin dhe analizimin e masave të marra nga institucionet përgjegjëse DPT, AKSHI, AKSK mbi funksionimin dhe sigurinë kibernetike të sistemit elektronik të tatimeve e-Taxation.
Auditimi i sigurisë kibernetike për infrastrukturën kritike e-Taxation evidentoi disa çështje kryesore që lidhen me përmirësimin e kuadrit ligjor e rregullator, ndarjen e përgjegjësive institucionale dhe zbatimin e masave të sigurisë, rritjes së bashkëpunimit dhe koordinimit të bashkëpunimit organizativ dhe teknik ndërmjet institucioneve DPT, AKSHI dhe AKSK, si dhe rritjes së kapaciteteve teknike dhe njerëzore të reagimit ndaj incidenteve.

Rregullorja e miratuar nga Autoriteti Kombëtar i Sigurisë Kibernetike me urdhrin nr. 97 datë 05.03.2024, mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit v3.0, përcakton që DPT është Operatori Administrues për e-Taxation, që ka dhe detyrimin për dokumentimin dhe zbatimin e masave të Sigurisë Kibenretike. Si operator i infrastrukturës kritike e-Taxation, DPT nuk mund të zbatojë masat e sigurisë kibernetike të parashikuara në Ligjin nr. 25/2024 dhe aktet nënligjore.
Drejtoria e Përgjithshme e Tatimeve, megjithëse ka detyrimin ligjor për menaxhimin e regjistrave të të dhënave, i mungojnë mekanizmat ligjorë dhe teknikë për ta realizuar si dhe roli dhe kompetencat në këtë drejtim.

Metodologjia për identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, nuk është hartuar ende. Aktet ligjore ne fuqi deri në fund të auditimit, e përcaktojnë sistemin e-Taxation si të rëndësishëm dhe jo kritik. Për këtë KLSH ka rekomanduar në auditimet e mëparshme riklasifikimin e tij si infrastrukturë kritike.

Nga analiza e masave organizative të marra për parandalimin e cenimeve kibernetike, u evidentua se distanca gjeografike ndërmjet qendrës primare dhe asaj sekondare nuk është në përputhje me standardet më të mira të sigurisë, duke krijuar një risk në rast të fatkeqësive natyrore. Nuk u konstatua ndonjë plan i strukturuar trajnimi për punonjësit e përfshirë në menaxhimin e sigurisë kibernetike, si dhe strukturat organizative të AKSHI-t përgjegjëse për monitorimin dhe mbrojtjen kibernetike nuk janë të kompletuara me staf, duke ndikuar në nivelin e përgjithshëm për mbrojtjen ndaj kërcënimeve kibernetike.

Në aspektin e masave teknike të sigurisë, u evidentuan disa incidente kibernetike të regjistruara gjatë viteve 2023-2024, duke përfshirë ekspozimin dhe keqpërdorimin e kredencialeve, aksesin e paautorizuar, rrjedhjen e të dhënave dhe sulmet malware. Kontrolli i aksesit mbetet një sfidë, pasi janë identifikuar raste të përdorimit të kredencialeve administrative në mënyrë të paautorizuar, duke rritur rrezikun e sulmeve të brendshme dhe të jashtme. Mungesa e enkriptimit për bazat e të dhënave e bën informacionin e ndjeshëm të cenueshëm ndaj shkeljeve të mundshme, ndërsa mungesa e një skedulimi të qartë për shqyrtimin e logeve të sistemit ndikon në aftësinë për të zbuluar dhe adresuar në kohë incidentet kibernetike.

1. PROBLEMI SOCIAL DHE RËNDËSIA E AUDITIMIT
1.1 Konteksti i problemit social

Me zhvillimin e shpejtë të teknologjisë së informacionit dhe përdorimit të tij në administratën publike, rëndësia e sigurisë kibernetike është rritur ndjeshëm në nivel global, duke prekur aspekte të ndryshme të jetës sociale, ekonomike dhe institucionale të vendeve të ndryshme. Në dekadat e fundit, me rritjen e përdorimit të sistemeve digjitale në sektorë si financat, shëndetësia dhe tatimet, siguria e të dhënave dhe infrastrukturave kritike është bërë një nga çështjet më të rëndësishme për qeveritë dhe organizatat ndërkombëtare.

Në vitet 1990, me fillimin e epokës së internetit dhe zgjerimin e teknologjisë, siguria kibernetike u pa fillimisht si një çështje teknologjike, që lidhej me mbrojtjen e rrjeteve dhe sistemeve nga sulmet e jashtme. Megjithatë, me kalimin e kohës, ndërhyrjet kibernetike janë bërë më të sofistikuara dhe më të shpeshta, duke përfshirë jo vetëm kriminelët kibernetikë por edhe aktorë shtetërorë, të cilët përdorin sulmet kibernetike për qëllime politike dhe ekonomike. Sulme si ai ndaj Estonisë në vitin 2007, i cili çoi në ndërprerjen e plotë të shërbimeve digjitale të vendit për disa ditë, ose sulmi ndaj sistemit të shëndetit të Mbretërisë së Bashkuar në 2017 (WannaCry), e kanë ngritur nivelin e ndërgjegjësimit për rëndësinë e masave të fuqishme të sigurisë kibernetike.

Në Shqipëri kanë ndodhur disa sulme kibernetike të rëndësishme vitet e fundit, që kanë vënë në dukje dobësitë e sistemeve të sigurisë kibernetike dhe kanë shtuar nevojën për masa më të forta mbrojtëse. Disa nga sulmet më të njohura janë:

- **Sulmi ndaj sektorit bankar (2016)**

Një tjetër incident i njohur ka ndodhur në vitin 2016, kur disa banka në Shqipëri u përballën me një seri sulmesh kibernetike që synonin të vjedhin të dhëna financiare dhe personale të klientëve. Këto sulme shkaktuan shqetësime në lidhje me sigurinë e sistemit bankar dhe rëndësinë e ruajtjes së integritetit të të dhënave financiare në sektorin privat.

- **Sulmi ndaj institucioneve shtetërore (2022)**

Një nga sulmet më të mëdha dhe më serioze ndodhi në korrik 2022, kur Shqipëria u përball me një sulm të fuqishëm kibernetik që synoi një numër të madh institucionesh shtetërore. Sistemi online i e-Albania-s, i cili përdoret nga qytetarët për të aksesuar dhe marrë shërbime publike, u ndërpre për disa ditë. Sulmi i atribuohej një grupi të lidhur me një shtet të huaj dhe qëllimi kryesor i tij ishte destabilizimi i qeverisë shqiptare dhe krijimi i kaosit në administratë. Ky sulm solli ndërprerjen e përkohshme të shumë shërbimeve digjitale dhe nxori në pah dobësitë e infrastrukturës kibernetike të vendit.

- **Sulmi ndaj sistemit TIMS (2022)**

Pas sulmit të parë në korrik, një tjetër sulm i rëndësishëm ndodhi në shtator 2022, kur sistemi TIMS (Sistemi i Menaxhimit të Informacionit për Policinë Kufitare) u shënjestrua. Ky sistem është kritik për menaxhimin e të dhënave të hyrje-daljeve në kufijtë e Shqipërisë dhe përdoret nga policia kufitare. Ndërprerja e tij ndikoi në sigurinë kombëtare dhe në funksionimin e përditshëm të kontrollit kufitar, duke shkaktuar vonesa dhe çrregullime në pikat kufitare të vendit.

Në Shqipëri, ashtu si në shumë vende të tjera, sfidat në mbrojtjen e infrastrukturës kritike kanë qenë një prioritet. Sistemet e menaxhimit të të ardhurave dhe financave publike, si sistemi E-Taxation, janë shënjestra të mundshme për sulme kibernetike duke synuar destabilizimin e administratës fiskale, vjedhjen e të dhënave financiare apo manipulimin e transaksioneve. Në një botë gjithnjë e më të ndërvarur nga teknologjia, pasojat e një sulmi të suksesshëm mund të jenë katastrofike, duke prekur besimin e publikut, stabilitetin ekonomik dhe funksionimin e qeverisë.

Duke qenë pjesë e një tregu global digjital, Shqipëria ka pasur të njëjtat sfida si shumë vende të tjera për të siguruar që infrastrukturat e saj kritike të mbrohen nga rreziqet kibernetike. Autoriteti Kombëtar i Sigurisë Kibernetike (AKSK) dhe Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) kanë një rol të rëndësishëm në zhvillimin e politikave dhe standardeve të sigurisë që mbrojnë këto sisteme nga sulmet e mundshme. Megjithatë, sfidat mbeten të mëdha, duke pasur parasysh zhvillimet e vazhdueshme në teknikat e sulmeve kibernetike dhe rritjen e ndërgjegjësimit mbi rëndësinë e ruajtjes së integritetit të të dhënave.

Në këtë kuadër, administrata tatimore në Shqipëri dhe sistemi E-Taxation kërkojnë masa të forta mbrojtëse, për të siguruar që qytetarët dhe bizneset të kenë besim në sigurinë e të dhënave të tyre financiare. Sulmet kibernetike në sektorin e tatimeve mund të shkaktojnë humbje të mëdha financiare, të dëmtojnë stabilitetin e tregut dhe të ulin besimin në institucionet shtetërore, duke prekur drejtpërdrejt mirëqenien e shoqërisë dhe të ekonomisë së vendit.

1.2 Rëndësia e auditimit të performancës

Auditimet e performancës vlerësojnë nëse synimet e politikave dhe skemat qeverisëse lidhen me problemet reale të shoqërisë dhe shqetësimet e palëve të interesit, duke dhënë një informacion shumë më të gjerë mbi ecurinë e të gjithë projekteve dhe programeve në entet publike të audituara. Këto auditime kryhen duke u bazuar tek Standardet Ndërkombëtare ISSAI dhe Udhëzuesi i Auditimit të Performancës (ISSAI 300, 3000, 3100, 3200, 5100 dhe 5200), Manuali i Auditimit të Performancës, Indikatorët e Performancës sipas praktikave më të mira audituese, të cilat shërbejnë si udhërrëfyes për konceptimin, planifikimin, kryerjen, konkludimin dhe ndjekjen e rekomandimeve të auditimit të performancës. Kontrolli i Lartë i Shtetit, duke synuar realizimin e misionit të tij, si institucion që ofron një ekspertizë të pavarur në ndihmë të një menaxhimi sa më të përgjegjshëm në shërbim të qytetarëve, jep një informacion shumë më të gjerë mbi ecurinë e të gjitha projekteve dhe programeve të institucioneve dhe enteve publike të audituara. Nëpërmjet auditimit të performancës synohet të analizohet ekonomiciteti, eficienca dhe efektiviteti i programeve të ekzekutivit. KLSH, nëpërmjet këtij auditimi, synon të paraqesë situatën aktuale në lidhje me sigurinë kibernetike të sistemit E-Taxation dhe do të ndihmojë në vlerësimin e masave të ndërmarra nga institucionet e përfshira dhe identifikimin e dobësive që mund të kenë ndikim të konsiderueshëm në jetën e qytetarëve dhe në stabilitetin e sistemeve financiare të vendit. Kështu, ky auditim ka një rëndësi të madhe për sigurinë e përgjithshme të sistemit tatimor dhe për krijimin e besimit të qytetarëve në administratën publike dhe në mbrojtjen e të dhënave të tyre nga rreziqet kibernetike.

1.3 Auditime të mëparshme apo aktuale në këtë fushë

Kontrolli i Lartë i Shtetit, në veprimtarinë e tij audituese nëpërmjet Departamentit të Auditimit të Teknologjisë së Informacionit, gjatë viteve të fundit i ka kushtuar një rëndësi gjithmonë e më të madhe auditimit të sistemeve dhe infrastrukturës IT të institucioneve publike me synim rritjen e llogaridhënies për qytetarët. Nën lupën e vlerësimeve të këtyre sistemeve gjatë viteve të fundit kanë qenë institucione kyçe që mbartin sisteme të rëndësishme dhe ofrojnë shërbime publike jetike për qytetarët, si: AKSHI, DPSHTRR, FSDKSH, UKT, RTSH, ASHK, APP, Posta Shqiptare etj.
Në Drejtorinë e Përgjithshme të Tatimeve vlen të përmendet:

- Auditimi IT me objekt "Auditimi i sistemeve të teknologjisë së informacionit në DPT" bazuar në programin e auditimit nr. 359/1, me datë 27.04.2023, i cili konkludoi me Vendimin e Kryetarit të KLSH nr. 158, datë 13.09.2023. Ky auditim u ushtrua pranë Drejtorisë së Përgjithshme të Tatimeve dhe arriti në përfundimin, ndër të tjera, se në aktet ligjore mbi infrastrukturat kritike, AKSHI dhe AKCESK (tani AKSK), nuk e kanë vlerësuar me rendësi kritike sistemin e-Taxation, duke mos krijuar kushtet për përmbushjen në kohë të detyrimeve për sigurinë kibernetike të kësaj infrastrukture. Nga ana e saj, u konkludua gjithashtu, DPT duhet të luajë një rol aktiv në lidhje me TI, për sa kohë në sistemet informatike kryhen veprime nga përdorues të brendshëm dhe të jashtëm dhe të dhënat e sistemeve janë tregues i aktivitetit të institucionit.

Marrë shkas nga gjetjet e mëparshme dhe zhvillimet në sigurinë kibernetike, ky auditim do të ketë në fokus pikërisht sigurinë kibernetike të sistemit E-Taxation.

2. SUBJEKTET NËN AUDITIM

2.1 Hyrje në subjektet nën auditim

Subjektet që do të përfshihen në këtë auditim janë:

1. Drejtoria e Përgjithshme e Tatimeve;
2. Agjencia Kombëtare e Shoqërisë së Informacionit;
3. Autoriteti Kombëtar për Sigurinë Kibernetike.

Drejtoria e Përgjithshme e Tatimeve

Drejtoria e Përgjithshme e Tatimeve administron mbledhjen e të ardhurave tatimore dhe kontributeve shoqërore, duke nxitur përmbushjen vullnetare dhe duke kërkuar nga të gjithë kuptimin dhe respektimin e detyrimeve ligjore. Drejtoria e Përgjithshme e Tatimeve është autoriteti shtetëror i specializuar, në varësi të Ministrisë së Financave për krijimin, sigurimin dhe mbledhjen e të ardhurave tatimore dhe Kontributeve të sigurimeve shoqërore dhe shëndetësore në Republikën e Shqipërisë. DPT ka funksionuar me rregulloren e miratuar me urdhrin nr. 193, datë 12.08.2020 të Ministrit të MFE, "Rregullorja e Funksionimit të Administratës Tatimore Qendrore", në të cilën trajtohen objekti dhe funksionet e punës për të gjithë strukturën përbërëse të DPT-së, Zhvillimi i teknologjisë së informacionit në DPT ka pësuar ndryshime të rëndësishme gjatë këtyre viteve. Sistemet informatike janë shumë të rëndësishme në DPT pasi aty mbështetet aktiviteti institucional dhe arritja e objektivave.

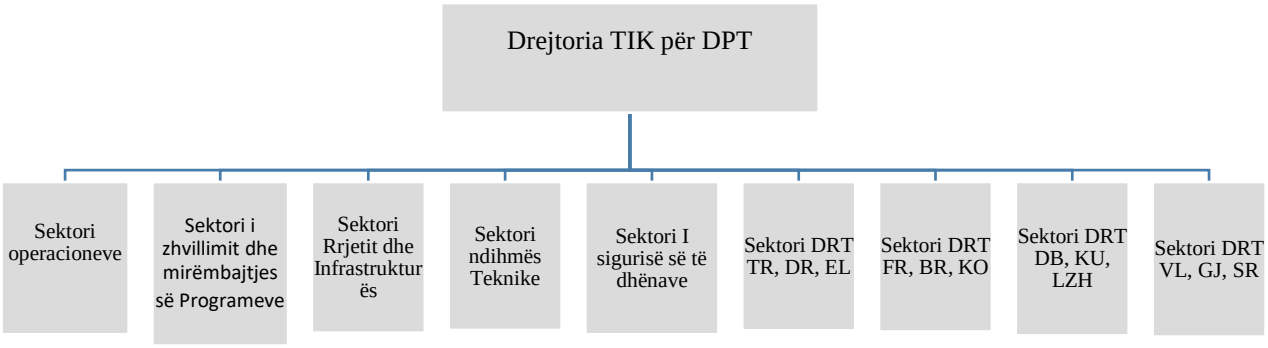
Funksionet kryesore të punës të Drejtorisë së Përgjithshme të Tatimeve janë si më poshtë:

- Administron detyrimet tatimore në Republikën e Shqipërisë në nivel qendror për llojet e tatimeve dhe taksave të përcaktuara në ligjin nr. 9920, datë 19.05.2008 "Për Procedurat Tatimore në Republikën e Shqipërisë", i ndryshuar, si dhe kontributet e sigurimeve shoqërore e shëndetësore të përcaktuara me ligjin nr. 9136, datë 11.09.2003 "Për Mbledhjen e Kontributeve të Detyrueshme të Sigurimeve Shoqërore e Shëndetësore në Republikën e Shqipërisë", i ndryshuar;
- Përgatit dhe miraton planin strategjik të objektivave dhe synimeve kryesore të administratës tatimore qendrore për një periudhë afat-shkurtër, afat-mesme dhe afat-gjatë si edhe monitoron zbatimin e tij.
- Evidenton nevojat për ndryshime dhe paraqet propozimet përkatëse në Ministrinë e Financave dhe Ekonomisë, lidhur me ndryshimet në ligjet tatimore, në aktet nën-ligjore të nxjerra në zbatim të tyre.
- Përgatit dhe miraton procedura standarde pune operative, ku sigurohet se këto procedura promovojnë transparencën e duhur në marrëdhëniet e administratës tatimore me tatimpaguesit, krijojnë sisteme të kontrollit të brendshëm të cilat minimizojnë rrezikun e korrupsionit, sigurojnë trajtim të paanshëm për të gjithë tatimpaguesit dhe reduktojnë subjektivitetin e punonjësve tatimorë.
- Ofron asistencë për të siguruar zbatimin korrekt të legjislacionit tatimor, akteve nën-ligjore në zbatim të tij dhe manualeve operacionale në Drejtoritë Rajonale Tatimore.
- Përcakton, në përputhje me dispozitat e legjislacionit të shërbimit civil, masa uniforme për matjen e performancës së punonjësve të administratës tatimore dhe krijon raporte standarde për të kontrolluar vlerësimin e performancës në nivel kombëtar, si dhe për çdo Drejtori 13 Rajonale Tatimore. Ndjek zbatimin e kërkesave të Kodit të Etikës për Administratën Tatimore Qendrore.
- Siguron shpërndarje të drejtë të burimeve njerëzore në çdo Drejtori Rajonale Tatimore.
- Bashkëpunon me të gjitha Drejtoritë Rajonale Tatimore, për të përgatitur plane vjetore pune, bazuar në numrin e personelit që është përcaktuar për çdo drejtori dhe në objektivat funksionale të performancës për çdo Drejtori Rajonale Tatimore.
- Harton dhe zbaton një program vjetor të vizitave të punës në çdo Drejtori Rajonale Tatimore, për të ofruar asistencë dhe për të kryer vlerësime.

- Miraton planin vjetor të punës dhe planin e të ardhurave tatimore për çdo Drejtori Rajonale Tatimore.
- Përgatit, miraton dhe kontrollon zbatimin e Kodit të Etikës për punonjësit e administratës tatimore, në përputhje me rregullat e etikës së administratës publike.
- Përgatit, miraton dhe kontrollon zbatimin e Rregullores së Brendshme të Administratës Tatimore Qendrore për parandalimin e konfliktit të interesit të nëpunësit të Administratës Tatimore qendrore.

Me Urdhër të Kryeministrit nr.13, datë 25.01.2024 "Për miratimin e strukturës dhe të organikës së Agjencisë Kombëtare të Shoqërisë së Informacionit", është miratuar struktura TIK për DPT si në figurën më poshtë.

Figura 1: Organograma e Drejtorisë TIK të AKSHI-t për DPT-ën



Burimi: AKSHI, Përpunoi: Grupi i auditimit

Në strukturën e miratuar për DPT me urdhër të Kryeministrit nr. 69, datë 26.05.2023 "Për miratimin e strukturës organizative dhe të numrit të përgjithshëm të personelit të administratës Tatimore Qendrore ", është shtuar një strukturë e re, emërtuar si Drejtoria e Administrimit të të Dhënave e cila ka për mision mirë administrimin e të dhënave në sistemet IT të administratës Tatimore në funksion të arritjes së objektivave operacionale dhe objektivave të përcaktuara në planin strategjik të institucionit. Detyrat kryesore janë:
- Rishikon rregulloret e dedikuara për administrimin e çdo sistemi informatik;
- Në bashkëpunim me drejtorinë TIK të AKSHI-t pranë DPT harton Strategjitë e *Backup* dhe Strategjitë e rikuperimit nga për çdo sistem dhe merr masa në vazhdimësi për implementimin dhe monitorimin e saj;
- Vlerëson dhe rekomandon zgjidhje teknike për çështje/incidentet dhe kërkesat e ardhura në lidhje me programet e sistemeve Informatike;
- Klasifikon problemet sipas llojit, impaktit, urgjencës dhe prioritetit nëpërmjet mbajtjes së një regjistri;
- Përgatit specifikimet teknike të prokurimeve mbi pajisjet kompjuterike dhe programet.

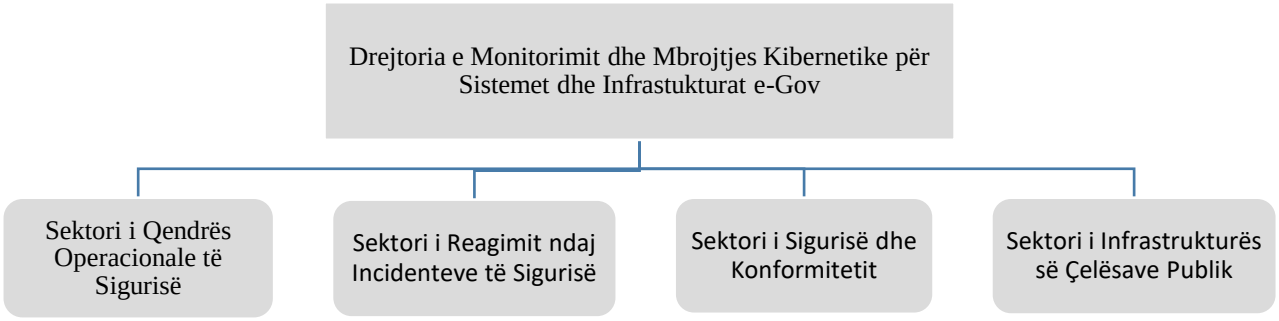
Agjencia Kombëtare e Shoqërisë së Informacionit

Agjencia Kombëtare e Shoqërisë së Informacionit është person juridik publik, i cili vepron në bazë të Kushtetutës, legjislacionit në fuqi, marrëveshjeve ndërkombëtare të nënshkruara, programit të qeverisë në fushën e shoqërisë së informacionit dhe në përmbushje të detyrave funksionale të ngarkuara AKSHI-it me VKM-në nr. 673 datë 22.11.2017

Në skemën më poshtë paraqitet struktura e Drejtorisë së Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-Gov, e miratuar me Urdhër të Kryeministrit nr.13, datë 25.01.2024 "Për miratimin e strukturës dhe të organikës së Agjencisë Kombëtare të Shoqërisë së Informacionit".

AKSHI me rregulloren nr.2, datë 06.11.2023 “Për Sigurinë e Informacionit”, ka përcaktuar se kjo drejtori monitoron, analizon dhe trajton të gjithë incidentet kibernetike ku AKSHI operon. Ajo përbëhet nga 4 sektor: Sektori i Qendrës Operacionale të Sigurisë, Sektori i Reagimit ndaj Incidenteve të Sigurisë, Sektori i Sigurisë dhe Konformitetit, Sektori i Infrastrukturës së Çelësave Publik.

Figura 2: Organograma e AKSHI për Drejtorinë e Monitorimit dhe Mbrojtjes Kibernetike



Burimi: AKSHI, Përpunoi: Grupi i auditimit

AKSHI në funksion të përmbushjes së veprimtarisë së saj ushtron këto kompetenca kryesore:

- promovon teknologji të reja, harton strategji dhe plan veprimi për zbatimin e politikave në fushën e teknologjisë së informacionit e të komunikimit elektronik e-GOV;
- zhvillon politika e strategji në sektorin e shoqërisë së informacionit, dhe në veçanti të teknologjisë së informacionit dhe komunikimit si dhe nxit investimet në fushën e SHI-së;
- bashkërendon programe në fushën e SHI-së, si edhe jep kontribut në edukimin dhe nxitjen e përdorimit të TIK-ut nga publiku;
- garanton një nivel të lartë të sigurisë kibernetike dhe zgjidhjet ndaj Incidenteve të Sigurisë Kompjuterike duke bashkërenduar me "CSIRT", si Ekipi Përgjegjës ndaj Incidenteve të Sigurisë Kompjuterike për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave;
- është autoritet rregullator koordinues, përgjegjës, i bazave të të dhënave shtetërore; dhe riorganizon dhe menaxhon strukturat përgjegjëse TIK, në institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave;
- ofron shërbime të përqendruara përmes teknologjisë së informacionit e komunikimit (T1K) për qeverisjen elektronike, për administratën shtetërore, qytetarët, bizneset;
- ofron shërbimin e nënshkrimit elektronik, së bashku me pajisjen përkatëse dhe vulën dixhitale, për organet dhe institucionet e administratës publike dhe subjektet private, sipas tarifave të përcaktuara në Vendimin e Këshillit të Ministrave; Përcaktimi i tarifave sipas kësaj shkronje bëhet me propozimin e AKSHI-t dhe miratimin e ministrit përgjegjës për Financat dhe Ekonominë;
- ngre dhe ofron shërbime elektronike për sportelet fizike të institucioneve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, të cilat ofrojnë shërbime publike;
- ofron sisteme IT, infrastrukturë hardware dhe TIK për ADISA në kuadër të ofrimit të shërbimeve publike në sportele fizike nga ana e saj; ngre, mirëmban dhe administron sistemeve dhe aplikacione të teknologjisë së informacionit dhe komunikimit, infrastrukturën e qendërzuar dhe infrastrukturën TIK përfshirë edhe ato të klasifikuara si sekret shtetëror, për institucionet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave;
- organizon, kryen prokurimet e përqendruara dhe lidh kontratat për pajisjet TIK përfshirë edhe ato të klasifikuara si sekret shtetëror, për institucionet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave;
- përcakton standardet shqiptare të TIK-ut, në përputhje me standardet ndërkombëtare dhe evropiane, të adoptuara, të cilat do të ndiqen nga administrata shtetërore. Këto standarde botohen në Buletinin e Njoftimeve Publike;

- gjithashtu referuar Strategjisë Kombëtare për Sigurinë Kibernetike, Agjencia Kombëtare e Shoqërisë së Informacionit, aplikon të gjitha masat e sigurisë konform legjislacionit në fuqi dhe standardit ISO 27001.

Autoriteti Kombëtar për Sigurinë Kibernetike

Autoriteti Kombëtar për Sigurinë Kibernetike ka përgjegjësinë e mbikëqyrjes së zbatimit të ligjit nr.25/2024 "Për Sigurinë Kibernetike", siguron mbikëqyrjen dhe drejton të gjithë procesin e qeverisjes kibernetike, nëpërmjet masave të sigurisë kibernetike, proceseve të kontrollit dhe menaxhimit të riskut si dhe përdorimin e mjeteve dhe zgjidhjeve të duhura teknologjike.

Në skemën më poshtë paraqitet struktura e AKSK e cila ka si objekt të veprimtarisë së saj sigurimin e mirëqeverisjes së sigurisë kibernetike, monitorimit dhe identifikimin të infrastrukturave kritike dhe të rëndësishme të informacionit. Struktura aktuale e Autoritetit Kombëtar për Sigurinë Kibernetike është miratuar me Urdhër të Kryeministrit nr.233, datë 20.12.2023. Kjo drejtori përbëhet nga drejtori drejtorisë dhe tre sektor: Sektori i qeverisjes së sigurisë kibernetike dhe i kontrollit, sektori i zhvillimit strategjik komunikimit dhe identifikimit në infrastrukturë, sektori statistikës i modeleve dhe i analizës së indikatorëve.

Figura 3: Drejtoritë në funksion të Sigurisë Kibernetike në AKSK

Drejtor i Përgjithshëm	Drejtoria e Certifikimit, Politikave e Legjislacionit të Sigurisë Kibernetike
	Drejtoria e Analizës së Sigurisë Kibernetike
	Drejtoria e Monitorimit dhe Reagimit të Incidenteve, Qendrës Operacionale SOC C-Sirt
	Drejtoria e Analizës së Përputhshmërisë, Riskut dhe Kontrollit të Sigurisë Kibernetike

Burimi: AKSK, Përpunoi: Grupi i auditimit

Kompetencat e AKSK bazuar në ligjin nr.25/2024 "Për Sigurinë Kibernetike":

- vepron si pikë qendrore kontakti në nivel kombëtar dhe ndërkombëtar, si dhe koordinon e bashkërendon punën me institucionet e tjera në fushën e sigurisë kibernetike për zgjidhjen e incidenteve kibernetike;
- vepron në cilësinë e CSIRT-it Kombëtar dhe CERT-it;
- përcakton dhe kontrollon zbatimin e masave të sigurisë kibernetike, që duhet të aplikohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit;
- bashkëpunon dhe shkëmben informacione të rëndësishme me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me të dhënat në sisteme, kur ato janë të rrezikuara për shkak të një incidenti kibernetik;
- asiston operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në menaxhimin e incidenteve kibernetike;
- kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet informacioneve të marra nga platformat e jashtme të ngritura nga Autoriteti ose operatorët e infrastrukturave të informacionit, si dhe nga platformat e brendshme me kërkesë nga operatorët e infrastrukturave të informacionit, me qëllim evidentimin e parandalimin e veprimeve keqdashëse;
- vlerëson dhe analizon nivelin e sigurisë kibernetike të sistemeve të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet kontrolleve dhe simulimeve të vazhdueshme, si dhe përcakton masa shtesë për operatorët e infrastrukturave të informacionit për një reagim sa më të shpejtë dhe efikas ndaj incidenteve apo sulmeve kibernetike; Metodologjia për vlerësimin dhe analizimin e sigurisë kibernetike miratohet me vendim të Këshillit të Ministrave;

- regjistron organet e vlerësimit të konformitetit për sigurinë kibernetike për vlerësimin e masave të sigurisë kibernetike;
- krijon dhe administron regjistrin e dokumentimit të incidenteve të sigurisë kibernetike;
- raporton në mënyrë periodike në lidhje me incidentet kibernetike pranë ENISA-s dhe organizmave të tjerë ndërkombëtarë në kuadër të angazhimeve të Republikës së Shqipërisë për çështjet e sigurisë kibernetike;
- kryen aktivitete ndërgjegjësimi në fushën e sigurisë kibernetike për të gjitha grupet e shoqërisë;
- autoriteti, me urdhër të drejtorit të përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, trajnime për personelin e këtyre operatorëve, në kuadër të përmbushjes me efektivitet të lartë të detyrave;
- ndërmerr masa të nevojshme, bashkëpunon dhe bashkërendon punën me institucionet përgjegjëse për sigurinë dhe mbrojtjen e fëmijëve dhe të rinjve për krijimin e një mjedisi *online* të sigurt kibernetik në Republikën e Shqipërisë.

2.2 Baza ligjore që rregullon çështjen nën auditim

Kriteret politike:

- Kushtetuta e Republikës së Shqipërisë.
- VKM nr. 1084, datë 24.12.2020, "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planit të veprimit 2020-2025";
- Standardi ndërkombëtar ISO 27001: 2022.
- Direktiva Evropiane NIS 2 - Network and Information Security.

Akte ligjore e nënligjore:

- Ligji nr. 25/2024 "Për Sigurinë Kibernetike";
- Ligji nr. 2/2017 "Për Sigurinë Kibernetike" (shfuqizuar);
- Ligji nr.9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar;
- Ligji nr. 43/2023 "Për qeverisjen elektronike";
- Ligji nr. 10325, datë 23.09.2010 "Për bazat e të dhënave shtetërore";
- VKM nr. 553, datë 15.7.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", ndryshuar me VKM nr. 761, datë 12.12.2022;
- VKM nr. 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit, i ndryshuar me VKM nr. 36, datë 24.1.2018 , me VKM nr. 448, datë 26.7.2018, me VKM nr.872, datë 24.12.2019;
- Rregullore për Kategorizimin e Incidenteve të Sigurisë Kibernetike (Miratuar me Urdhrin nr.299, datë 21.08.2024);
- Rregullore për Kategoritë e Incidenteve Kibernetike si dhe Formatin e Elementët e Raportit, miratuar me Urdhër nr. 62, datë 10.09.2018 të Drejtorit të Përgjithshëm të Autoritetit (shfuqizuar);
- Rregullore mbi Mënyrën e Dokumentimit dhe Implementimit të Masave të Sigurisë në Infrastrukturat Kritike dhe të Rëndësishme të Informacionit, miratuar me Urdhër Nr. 97, datë 05.03.2024 të Drejtorit të Përgjithshëm të AKSK;
- Rregullore mbi Përmbajtjen dhe Mënyrën e Dokumentimit të Masave të Sigurisë, miratuar me Urdhër nr.148, datë 20.07.2023, të Drejtorit të Përgjithshëm të Autoritetit, e ndryshuar;
- Rregullore e brendshme nr. 1900 prot., datë 16.04.2020 "Mbi detyrat dhe funksionimin e Agjencisë Kombëtare të Shoqërisë së Informacionit";
- Rregullore e Brendshme "Për organizimin dhe funksionimin e AKCESK", miratuar me Urdhrin nr. 201 , datë 20.11.2023 të Drejtorit të Përgjithshëm të Autoritetit;

- Rregullore e Brendshme "Për organizimin dhe funksionimin e AKCESK", miratuar me Urdhrin nr. 87, date 1.7.2020, të Drejtorit të Përgjithshëm të Autoritetit;
- Urdhër nr. 529, datë 06.11.2023, "Për miratimin e Rregullores për Sigurinë e Informacionit";

Praktika të mira ndërkombëtare:

- Raport auditimi i SAI-t norvegjez, OAGN, "Information security in research in the knowledge sector", publikuar më 17.01.2024;
- Raport auditimi i SAI-t suedez, Riksrevisionen, "Government control of national information and cyber security – both urgent and important (RiR 2023:8)", publikuar më 12.06.2023;
- Raport auditimi i SAI-t finlandez, NAOF, "Cyber protection arrangements", publikuar më 10.10.2017;
- Raport auditimi i SAI-t danez, Rigsrevisionen, "Report on the cyber security resilience of the public sector", publikuar më 04.11.2022 dhe "Report on the cyber security resilience of the Danish public sector II", publikuar më 04.12.2022".

2.3 Rëndësia e produkteve të subjektit

Strategjia Kombëtare për Sigurinë Kibernetike dhe Plani i Veprimit 2020 – 2025 janë miratuar nga Këshilli i Ministrave me Vendimin nr.1084, datë 24.12.2020.

Qëllimi i Ligjit nr.25/2024 "Për Sigurinë Kibernetike", është përcaktimi i masave të sigurisë me qëllim arritjen e një niveli të lartë të sigurisë kibernetike për rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë. Ky ligj ka si objekt përcaktimin e të drejtave dhe detyrimeve të subjekteve publike dhe private, të cilat administrojnë infrastruktura të informacionit, rrjetet e komunikimit dhe sistemet e tyre, cenimi apo shkatërrimi i të cilave do të kishte impakt në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.

Rëndësia e aktivitetit të Autoritetit Kombëtar për Sigurinë Kibernetike qëndron në përgjegjësinë e tij për të mbikëqyrur dhe garantuar sigurinë kibernetike në Republikën e Shqipërisë. Sipas ligjit për sigurinë kibernetike, ky institucion ka funksione të rëndësishme që ndikojnë në ruajtjen e integritetit dhe sigurisë së rrjeteve dhe sistemeve të informacionit, të cilat janë kritike për shëndetin publik, sigurinë ekonomike dhe funksionimin e ekonomisë dhe shoqërisë.

Në zbatim të detyrimeve ligjore dhe funksionale të Autoritetit Kombëtar për Sigurinë Kibernetike, janë identifikuar infrastrukturat kritike dhe miratuar me VKM nr. 553, datë 15.7.2020 "*Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit*", ndryshuar me VKM nr. 761, datë 12.12.2022.

Agjencia Kombëtare e Shoqërisë së Informacionit krijuar me VKM nr.673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit", e ndryshuar, është Agjencia Kombëtare për Shoqërinë e Informacionit – AKSH, ka një rëndësi të veçantë ku arsyet kryesore janë:

Modernizimi i Shërbimeve Publike: AKSHI është përgjegjës për zhvillimin dhe mirëmbajtjen e sistemeve dixhitale që mundësojnë ofrimin e shërbimeve publike online për qytetarët dhe bizneset. Platforma si "e-Albania" ka thjeshtuar aksesin dhe ofrimin e këtyre shërbimeve, duke reduktuar burokracinë dhe përmirësuar efikasitetin e administratës publike.

Menaxhimi i Infrastrukturës IT Shtetërore: AKSHI është institucioni kryesor për menaxhimin dhe mirëmbajtjen e infrastrukturës IT të administratës shtetërore. Kjo përfshin rrjetet, serverët, dhe qendrat e të dhënave ku ruhen informacionet e ndjeshme të qeverisë dhe qytetarëve.

Siguria Kibernetike: Si përgjegjëse për mbrojtjen dhe sigurinë e sistemeve IT të qeverisë, AKSHI luan një rol kyç në sigurimin e mbrojtjes kundër kërcënimeve kibernetike.

Zhvillimi i Strategjive Dixhitale: AKSHI luan një rol në hartimin e strategjive për digjitalizimin e vendit, duke ndihmuar vendin të përmirësojë kapacitetet teknologjike dhe të adaptojë praktikat e fundit në fushën e teknologjisë së informacionit dhe komunikimit.

Ndihma për Institucionet Publike: Përveç shërbimeve të drejtpërdrejta për qytetarët, AKSHI mbështet institucionet publike për zbatimin e projekteve dhe sistemeve dixhitale të nevojshme për funksionimin e tyre.

Drejtoria e Përgjithshme e Tatimeve është Operatori Administrues për sistemet tek të cilat bazohet aktiviteti i saj që janë Sistemi e-Taxation dhe Fiskalizimi, klasifikuar si kritike me VKM nr.553, datë 15.07.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", ndryshuar me VKM nr.761, datë 12.12.2022. Sistemi **e-Taxation** kontribuon në një administratë më transparente dhe efikase, ndërsa siguron që të ardhurat nga taksat të mblidhen në mënyrë të drejtë dhe të sigurt. Pa funksionimin e tij të vazhdueshëm dhe të mbrojtur, shteti do të përballej me vështirësi të mëdha në menaxhimin e financave publike dhe në ofrimin e shërbimeve publike jetësore. DPT nuk ka më një strukturë të vetën për teknologjinë e informacionit qe prej vitit 2018. Transferimi i infrastrukturës së teknologjisë së informacionit tek AKSHI, ku përfshihen jo vetëm pajisjet fizike servera, router etj., por dhe sistemet informatike që janë ndërtuar dhe janë funksionalë aktualisht, ka përfunduar në fund të vitit 2022.

Sistemi **e-Taxation** është një infrastrukturë kritike për shtetin shqiptar dhe për funksionimin e tij në mënyrë efikase dhe të sigurt. Rëndësia e këtij sistemi fokusohet në drejtim të:

*Lehtësimit të Procesit të Mbledhjes së Taks*ave: Sistemi **e-Taxation** dixhitalizon dhe automatizon proceset e mbledhjes së taksave. Duke qenë se të ardhurat nga taksat janë burimi kryesor për financimin e shërbimeve publike dhe infrastrukturës, funksionimi i pandërprerë dhe i sigurt i këtij sistemi është jetik për stabilitetin ekonomik të vendit.

Rritjes së Transparencës dhe Luftës Kundër Evazionit Fiskal: Dixhitalizimi i proceseve të taksave ndihmon në zvogëlimin e evazionit fiskal, duke regjistruar automatikisht të gjitha transaksionet dhe deklaratat tatimore, çfarë siguron një transparencë më të madhe në raportimin e detyrimeve dhe pagimin e taksave.

Ofrimit të shërbime më të Mira për Qytetarët dhe Bizneset: Sistemi **e-Taxation** u lejon qytetarëve dhe bizneseve të kryejnë proceset e tyre tatimore online, pa pasur nevojë të paraqiten fizikisht në zyrat e administratës tatimore.

Përmirësimit të Sigurisë dhe Reduktimit të Rrezikut të Korrupsionit: Duke qenë një sistem plotësisht dixhital, **e-Taxation** redukton ndërveprimin e drejtpërdrejtë ndërmjet individëve dhe punonjësve të administratës tatimore, çka mund të ulë rrezikun e korrupsionit.

Infrastrukturë Kritike për Stabilitetin Ekonomik: **e-Taxation** përfaqëson një infrastrukturë kritike pasi siguron funksionimin e pandërprerë të sistemit tatimor, që është një nga shtyllat kryesore të qëndrueshmërisë financiare të shtetit.

Integrimit me Sistemet e Tjera Shtetërore: **e-Taxation** është ndërlidhur me sisteme të tjera shtetërore, përfshirë regjistrat e bizneseve, regjistrin e popullsisë etj.

Mbrojtja nga Sulmet Kibernetike. Duke qenë një objektiv i rëndësishëm për hakerët dhe aktorët e këqij, sistemi e-Taxation kërkon masa të forta sigurie kibernetike për të mbrojtur të dhënat e ndjeshme dhe për të parandaluar ndërprerjen e shërbimeve. Siguria e tij është thelbësore për besimin e qytetarëve dhe për ruajtjen e stabilitetit fiskal të vendit.

Kontratat e shërbimit të implementimit dhe mirëmbajtjes janë zhvilluar nga AKSHI i cili është dhe Autoriteti Kontraktor, ndërsa për ndjekjen dhe zbatimin e tyre janë ngritur grupe të përbashkëta ndërmjet AK dhe institucionit përfitues që është DPT. Për mbarëvajtjen e shërbimeve TIK, është nënshkruar ndërmjet AKSHI-t dhe DPT-s një marrëveshje bashkëpunimi, protokolluar në AKSHI me shkresën nr. 1745/1 prot., datë 08.04.2019 dhe protokolluar në DPT me nr. 7160 prot., datë 05.04.2019, ku përcaktohet niveli i shërbimit që duhet t'i ofrohet Drejtorisë së Përgjithshme të Tatimeve.

2.4 Pesha në buxhet

Drejtoria e Përgjithshme e Tatimeve nuk ka planifikuar dhe shpenzuar fonde nga Buxheti i Shtetit në drejtim të Sigurisë Kibernetike, për periudhën janar 2023 - shtator 2024.

Agjencia Kombëtare e Shoqërisë së Informacionit ka planifikuar dhe shpenzuar nga buxheti në drejtim të Sigurisë Kibernetike, si më poshtë:

Tabela 1: Shpenzime nga AKSHI për periudhën janar 2023-shtator 2024 mbi Sigurinë Kibernetike

Nr	Emërtimi	Njësia	Plan	Fakt
1	Përmirësimi dhe Optimizimi i perimetrave të sigurisë për AKSHI, kontratë nr.46 prot, date 11.01.2023.	Lekë	163,655,972.4	163,655,972.4
2	Certifikimi me ISO 37001, ri kontrolli i standardeve ndërkombëtare ISO 27001, 9001, 20000-1 dhe auditimi për konformitet ndaj eIDAS për shërbimet e besuara, kontratë nr 9 prot, datë 17.05.2022.	Lekë	93.720.000	45.276.000
3	Rinovimi i shërbimit të mbrojtjes Kibernetike për rrjetin qeveritar, kontratë e klasifikuar nr5913 prot, datë 20.10.2023	Lekë	96.444.600	38.577.840

Burimi: AKSHI, Përpunoi: Grupi i auditimit

Autoriteti Kombëtar për Sigurinë Kibernetike ka planifikuar dhe shpenzuar nga buxheti në drejtim të Sigurisë Kibernetike ne vlerën dhe zërat e mëposhtëm:

Tabela 2: Shpenzime nga AKSK për periudhën janar 2023-shtator 2024 mbi Sigurinë Kibernetike.

Nr	Emërtimi	Njësia	Plan 2023	Fakt 2023	Plan 2024	Fakt Shtator 2024
1	Sistemi i kontrollit dhe vlerësimit të sigurisë kibernetike	Lekë	50,000,000	0	151,200,000	0
2	Sistemi i analizës së vulnerabiliteteve dhe Inteligjencës ndaj Kërcënimeve (Threat Intelligence).	Lekë	110,000,000	0	-	-
3	Përmirësim dhe shtim i funksionaliteteve të sistemit të menaxhimit dhe raportimit të incidenteve kibernetike.	Lekë	131,320,204	0	120,900,000	120,900,000
4	Ngritja e platformës së emulimit e-learning dhe stërvitjes kibernetike	Lekë	-	-	24,100,000	0
5	Produktet Teknologjike të Inteligjencës Artificiale për Sigurinë Kibernetike	Lekë	-	-	1,500,000,000	0

Burimi: AKSK, Përpunoi: Grupi i auditimit

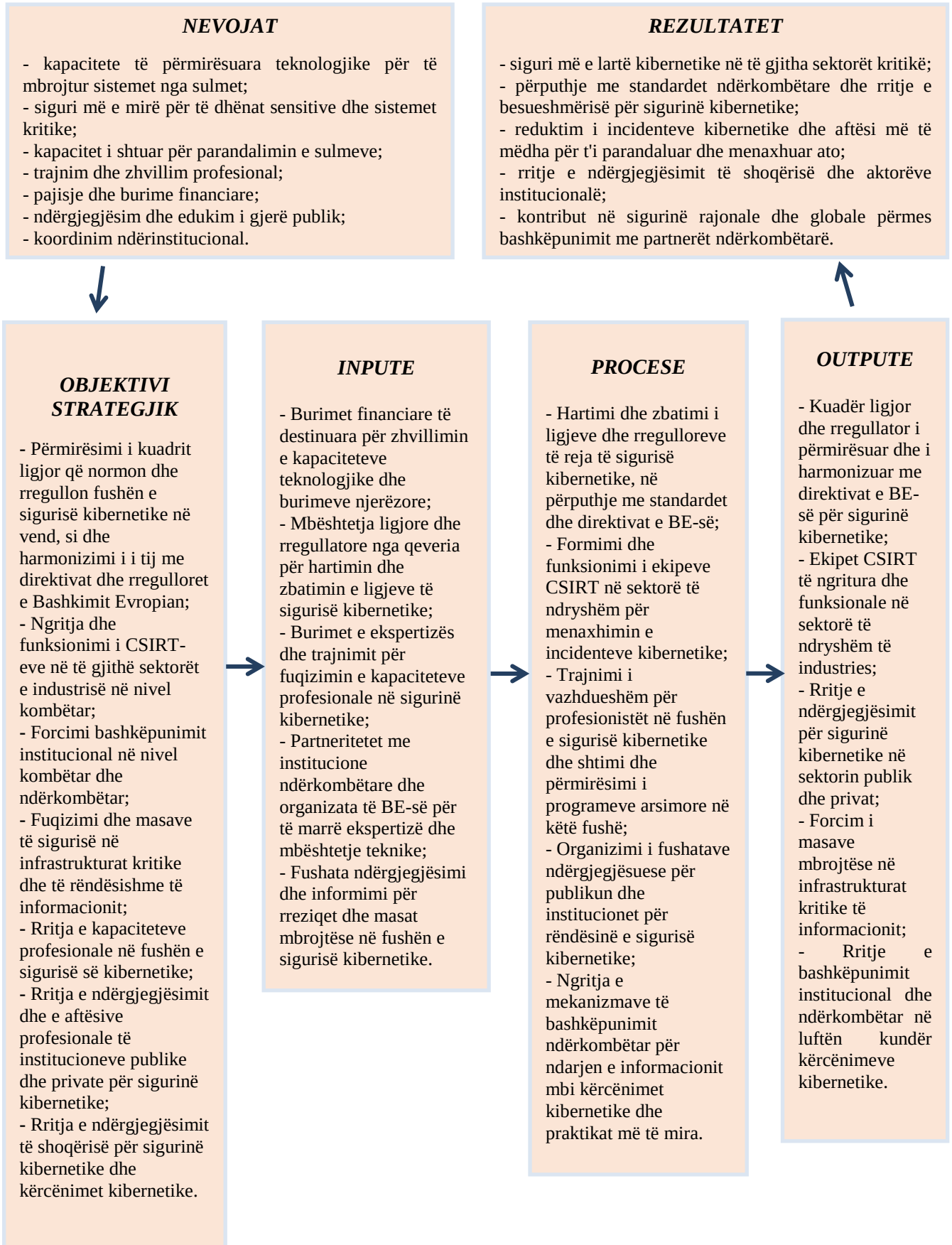
2.5 Përkufizimet dhe terminologjia

"**AKSHI**" është Agjencia Kombëtare e Shoqërisë së Informacionit.
"**Autoriteti Përgjegjës për Certifikimin Elektronik dhe për Sigurinë Kibernetike**", ose "**AKSK**", ose "**Autoriteti**" është institucioni përgjegjës, i krijuar në bazë të legjislacionit në fuqi për nënshkrimin elektronik.
"**Baza e të dhënave shtetërore**" është grumbullimi i organizuar i informacionit, i ruajtur në formë elektronike, ku përpunimi dhe përditësimi i tij kryhen nëpërmjet një sistemi kompjuterik, si pjesë e plotësimit të detyrimeve ligjore të institucionit administrues.
"**CSIRT**" është Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike.
"**DATI**" është Departamenti i Auditimit të Teknologjisë së Informacionit në KLSH.

"**Hapësirë kibernetike**" është mjedisi digjital i aftë të krijojë, të procesojë dhe të shkëmbejë informacionin e krijuar nga sistemet, shërbimet e shoqërisë së informacionit, si dhe rrjetet e komunikimit elektronik.
"**Incident i sigurisë kibernetike**" është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit dhe sjell një efekt real negativ.
"**Infrastruktura e ofrimit të shërbimeve elektronike**" është tërësia e pajisjeve fizike e sistemeve dhe infrastruktura fizike e ndërlidhur që mundëson ofrimin e shërbimeve elektronike.
"**Infrastrukturë e rëndësishme e informacionit**" është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik, i cili nuk është pjesë e infrastrukturës kritike të informacionit, por që mund të rrezikojë apo të kufizojë punën e administratës publike në rastin e cenimit të sigurisë së informacionit.
"**Infrastrukturë kritike e informacionit**" është tërësia e rrjeteve dhe sistemeve të informacionit, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
"**Operator i infrastrukturës kritike të informacionit**" është një person juridik, publik ose privat, që administron infrastrukturën kritike të informacionit.
"**Operator i infrastrukturës së rëndësishme të informacionit**" është një person juridik publik, që administron infrastrukturë të rëndësishme të informacionit.
"**Përdorues**" janë nëpunësit e autoriteteve publike, të cilët përdorin shërbime elektronike në kuadër të ushtrimit të kompetencave të tyre dhe shtetasi, personi fizik ose juridik që përdor shërbimet elektronike.
"**Rrezik i sigurisë kibernetike**" është një rrethanë ose një ngjarje, e identifikueshme në mënyrë të arsyeshme, e cila mund të shkaktojë cenimin e sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit.
"**Rrjet i komunikimit dhe sistem i informacionit**" do të thotë:
a) një rrjet i komunikimeve elektronike, në kuptimin e pikës 36, të nenit 3, të ligjit nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", të ndryshuar";
b) çdo pajisje ose grup i lidhur ose i ndërlidhur i pajisjeve, nga të cilat, një ose më shumë se një, në bazë të një programi, kryejnë përpunimin automatik të të dhënave digjitale; ose
c) të dhënat digjitale të ruajtura, të përpunuara, të gjetura ose të transmetuara nga elementet e parashikuara në shkronjat "a" dhe "b", të kësaj pike, për qëllim të funksionimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre.
"**Siguria e informacionit**" është sigurimi i konfidencialitetit, integritetit dhe disponueshmërisë së informacionit.
"**Siguria kibernetike**" është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike.
"**Siguria e sistemeve të informacionit**" është tërësia e masave, politikave, procedurave, teknologjia dhe masat e nevojshme për mbrojtjen e të dhënave/elementeve të sistemit të informacionit, por edhe tërë sistemit nga çdo kërcënim i qëllimshëm apo i rastësishëm.
"**TIK**" është teknologjia e informacionit dhe komunikimit.

2.6 Skema e analizës së programit auditues

*Skema 1:*Modeli Input – Output



2.7 Feedback-u i subjektit në fazën studimore

Gjatë fazës studimore, stafet përgjegjëse të DPT-së, AKSHI-t dhe AKSK-së i janë përgjigjur përgjithësisht në kohë pyetësorëve të dërguar nga grupi i auditimit, ndërsa për plotësimin e informacionit dhe dokumentacionit të kërkuar që lidhet me mbledhjen e të dhënave plotësuese mbi tregues dhe indikatorë të ndryshëm, kërkuan më shumë kohë në përgjigjet e tyre, kjo edhe për shkak të natyrës dhe kompleksitetit të informacioneve të kërkuara nga grupi i auditimit.

3. DETAJET E AUDITIMIT

3.1 Vlerësimi i risqeve të aktiviteteve të subjektit

Vlerësimi i risqeve të aktiviteteve e politikave të subjekteve të përfshira në këtë auditim, kanë të bëjnë me vështirësitë dhe pengesat që ato hasin në realizimin e detyrave dhe funksioneve të përcaktuara në kuadrin ligjor e rregullator në fuqi. Për të kryer analizën e riskut, jemi mbështetur në analizën SWOT duke marrë në konsideratë fuqitë, dobësitë, mundësitë dhe kërcënimet që paraqiten në veprimtarinë e subjekteve nën auditim, që lidhen me fushën e sigurisë kibernetike. Analiza SWOT është një kornizë që përdoret për të identifikuar dhe analizuar fuqitë, dobësitë, mundësitë dhe kërcënimet që paraqiten lidhur me çështjen që trajtohet. Analiza SWOT është e dizenjuar për të ofruar një qasje realiste, të bazuar në fakte dhe të dhëna e cila përdor burime të brendshme dhe të jashtme dhe përdoret si një teknikë për të vlerësuar performancën, risqet dhe mundësitë potenciale për zhvillim dhe arritjen e objektivave. Për kryerjen e analizës grupi i auditimit ka përcaktuar objektivin që synohet të arrihet përmes këtij auditimi, ka mbledhur të dhëna dhe evidenca dhe ka bashkërenduar mendimet dhe konceptet e secilit prej anëtarëve të grupit. U përzgjodh përdorimi i analizës SWOT nisur nga fakti që kjo analizë ofron mundësinë e një menaxhimi më efikas të një problemi kompleks siç është siguria kibernetike për mbrojtjen e të dhënave gjatë ofrimit të shërbimeve publike në mënyrë elektronike. Duke iu referuar evidentimit të fuqive, dobësive, shanseve dhe kërcënimeve të paraqitur në analizën SWOT, grupi i auditimit ka bërë një ndarje dhe grupim të risqeve të veprimtarisë së institucioneve përkatëse, për të adresuar dhe ndarë faktorët e riskut sipas përkatësisë së tyre, brenda kontrollit dhe jashtë kontrollit menaxherial.

Gjithashtu është bërë edhe kategorizimi i tyre në nivel strategjik, financiar, juridik dhe operacional.

Figura 4: Analiza SWOT

Fuqitë - S	**Dobësitë - W**
- Korniza rregullatore për Sigurinë Kibernetike; - Autoritet qendror për sigurinë kibernetike; - Infrastruktura qendrore Data Center; - AKSK dhe AKSHI kanë ekipe të specializuara për sigurinë kibernetike; - Sistem qendror për menaxhimin dhe mbledhjen e të dhënave financiare dhe tatimore;	- Burime të kufizuara në fonde; - Shumëllojshmëria e sistemeve dhe platformave të ndryshme; - Nevoja për ndryshime të shpeshta ligjore apo rregullatore; - Varësia nga AKSHI për disa elementë të Sigurisë Kibernetike;
Shanset - O	**Kërcënimet- T**
- Fokus i shtuar në Sigurinë Kibernetike; - Marrëveshje bashkëpunimi me institucione ndërkombëtare; - Financime nga Organizata Ndërkombëtare; - Zhvillimi i kapaciteteve organizative dhe teknike; - Rritja e ndërgjegjësimit publik;	- Kërcënimet Kibernetike janë në zhvillim të shpejtë, dhe me synime drejt të dhënave sensitive; - Mungesa e burimeve të mjaftueshme për tu përballur me kërcënimet; - Mungesa e bashkëpunimit dhe koordinimit ndërmjet institucioneve me role të ndryshme; - Harmonizimi i rregulloreve ndërkombëtare me ato kombëtare;

Tabela 3: Analiza e Riskut

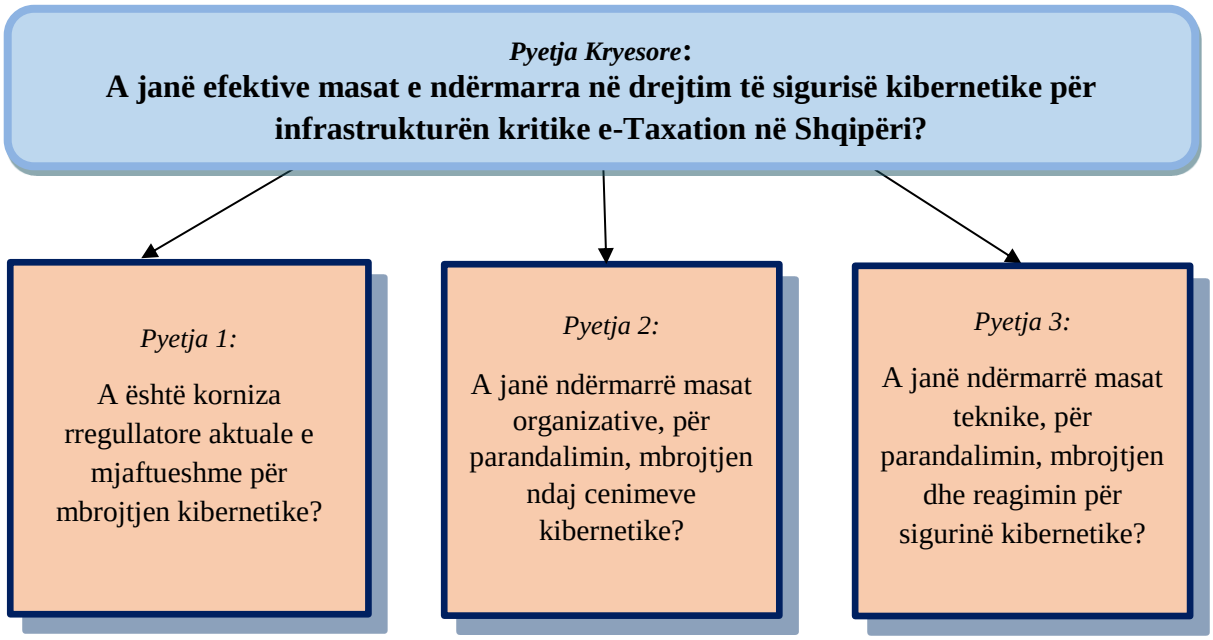
Nr.	Risku i Subjektit	Kategorizimi i riskut	Niveli i Riskut
1	Mungesa e një plani strategjik për mbrojtjen e infrastrukturave kritike të informacionit.	**Risk Strategjik**	I lartë
2	Një planifikim i dobët në infrastrukturën e sigurisë IT çon në mungesë të burimeve dhe teknologjive për të mbrojtur sistemet.		I mesëm
3	Shpenzime të mëdha për përputhshmërinë me standardet e sigurisë kibernetike mund të përbëjnë një risk të konsiderueshëm financiar për institucionet.	**Risk Financiar**	I lartë
4	Sulmet e suksesshme mund të çojnë në humbje të konsiderueshme financiare, për shkak të ndërprerjes së shërbimeve dhe riparimit të infrastrukturës së dëmtuar.		I lartë
5	Mosrespektimi i rregullave dhe ligjeve për mbrojtjen e të dhënave personale dhe sigurinë kibernetike mund të çojë në shkelje ligjore dhe penalitete.	**Risk Rregullator dhe Juridik**	I mesëm
6	Paqartësia e detyrimeve ligjore dhe nënligjore që mbulojnë sigurinë kibernetike mund të shërbejnë si rrezik në shkeljen e sigurisë së të dhënave.		I lartë
7	Kapacitetet teknike dhe burimet njerëzore të limituara mund të pengojnë aftësinë për të monitoruar dhe menaxhuar sigurinë.	**Risk Operacional**	I lartë
8	Një sistem i dobët monitorimi dhe reagimi ndaj incidenteve mund të lejojë sulmet të kalojnë pa u zbuluar për periudha të gjata kohore.		I lartë
9	Mungesa e bashkëpunimit efektiv ndërmjet institucioneve mund të vonojë identifikimin dhe përgjigjen ndaj kërcënimeve kibernetike.		I mesëm
10	Mungesa e kuptueshmërisë dhe zbatimit të protokolleve për menaxhimin e incidenteve, përbën risk që ndërhyrjet kibernetike të menaxhohen në mënyrë të paefektshme.		I mesëm

Burimi: Grupi i Auditimit

3.2 Objektivi i auditimit

Auditimi me temë "Siguria kibernetike e infrastrukturës kritike e-Taxation" ka si objektiv kryesor vlerësimin dhe analizimin e masave të marra nga institucionet përgjegjëse (DPT, AKSHI, AKSK) mbi funksionimin dhe sigurinë kibernetike të sistemit elektronik të tatimeve. Gjithashtu, do të shqyrtohet impakti që ky sistem ka në efektivitetin administrativ, sigurinë e të dhënave tatimore dhe besimin e qytetarëve e bizneseve ndaj shërbimeve publike. Në këtë mënyrë synohet të sigurohet një vlerësim i paanshëm dhe objektiv mbi veprimet dhe politikat e ndërmarra nga institucionet e audituara në lidhje me sigurinë kibernetike dhe funksionimin e sistemit E-Taxation. Përmes këtij objektivi, është konkluduar mbi efektivitetin e veprimtarisë së institucioneve subjekt auditimi për periudhën 01.01.2023 - 30.09.2024.

3.3 Pyetjet e auditimit



3.4 Fushëveprimi i auditimit

Ky auditim ka patur si fushëveprim analizimin dhe dhënien e një opinioni mbi efektivitetin e institucioneve, si dhe respektimin e kritereve ligjore e rregullatore, me qëllim arritjen e një niveli të lartë të sigurisë kibernetike, përfshirë masat e nevojshme të sigurisë, të të drejtave dhe detyrimeve të subjekteve, si dhe promovimin e bashkëpunimit të ndërsjellë ndërmjet aktorëve që operojnë në këtë fushë. Më konkretisht, mbi besueshmërinë dhe sigurinë në transaksionet elektronike ndërmjet qytetarëve, bizneseve dhe autoriteteve publike, duke kontribuar në rritjen e efektivitetit të shërbimeve publike dhe private, si dhe tregtisë elektronike. Për më tepër, ajo përcakton standardet minimale teknike për sigurinë e të dhënave dhe rrjeteve/sistemeve të informacionit, në përputhje me standardet ndërkombëtare, me synimin për të krijuar një mjedis elektronik të sigurt dhe të besueshëm.
Institucione subjekt auditimi ka patur DPT, AKSHI si dhe AKSK, sa i përket vlerësimit të performancës dhe kontrollit dhe respektimit të kritereve ligjore e rregullatore me qëllim përmirësimin e sigurisë kibernetike.
Periudhë objekt auditimi siç është theksuar dhe më sipër ka patur 2023 - 2024, megjithatë të dhëna historike jashtë kësaj periudhe mund të pasqyrohen për të ofruar një panoramë më të qartë të ecurisë së treguesve të ndryshëm dhe performancës.

4. SHTJELLIMI I PYETJEVE AUDITUESE

Pyetja kryesore: A janë efektive masat e ndërmarra në drejtim të sigurisë kibernetike për infrastrukturën kritike e-Taxation në Shqipëri?

Mesazhi i auditimit

Megjithëse janë ndërmarrë hapa të rëndësishëm drejt përmirësimit të sigurisë kibernetike në Shqipëri, auditimi vuri në dukje nevojën e menjëhershme për forcimin dhe harmonizimin e kuadrit ligjor e rregullator, në veçanti përsa i përket zbatimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit.
Mospërputhjet ligjore, mungesa e trajnimeve dhe e dokumentacionit për përdoruesit fundorë, si dhe boshllëqet në burimet njerëzore të specializuara, si në Drejtorinë e Monitorimit dhe Mbrojtjes Kibernetike ashtu edhe në sektorin e Sigurisë së të Dhënave, rrisin ndjeshëm ekspozimin ndaj risqeve kibernetike dhe kufizojnë kapacitetin reagues ndaj incidenteve.
Në aspektin teknik, auditimi identifikoi mungesë dokumentacioni dhe kontrolle të pamjaftueshme mjedisore në rast përmbytjesh apo zjarresh në Data Center-in Qeveritar. Po ashtu, në sistemin e-Taxation, mungesa e enkriptimit të të dhënave, shqyrtimi jo i rregullt i log-eve dhe mungesa e kontrolleve për aksesin e jashtëm e palët e treta, paraqesin një kërcënim për sigurinë e informacionit.

4.1 A është korniza rregullatore aktuale e mjaftueshme për mbrojtjen kibernetike?

Për përmirësimin e Sigurisë Kibernetike në Shqipëri, janë ndërmarrë hapa të rëndësishëm në drejtim të përmirësimit të kuadrit ligjor, çfarë është e domosdoshme me teknologjinë e informacionit që kemi zhvilluar në 10 vjeçarin e fundit e shoqëruar dhe me rritjen e numrit të shërbimeve publike që ofrohen në distancë (online).
Aktet ligjore ku bazohet Siguria Kibernetike për infrastrukturat kritike në të cilat bën pjesë dhe infrastruktura e sistemit e-Taxation, do të analizohen në vijim.

Ligji për Sigurinë Kibernetike nr. 25/2024.

Kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike, renditen në nenin 9 të këtij ligji, ku disa nga detyrat kryesore që lidhen me objektin e auditimit janë:

- Pika a - identifikon dhe klasifikon infrastrukturat kritike dhe të rëndësishme të informacionit.
- Pika ç - përcakton dhe kontrollon zbatimin e masave të sigurisë kibernetike, që duhet të aplikohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.
- Pika d - bashkëpunon dhe shkëmben informacione të rëndësishme me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me të dhënat në sisteme, kur ato janë të rrezikuara për shkak të një incidenti kibernetik.
- Pika dh - asiston operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në menaxhimin e incidenteve kibernetike.
- Pika ë - vlerëson dhe analizon nivelin e sigurisë kibernetike të sistemeve të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet kontrolleve dhe simulimeve të vazhdueshme, si dhe përcakton masa shtesë për operatorët e infrastrukturave të informacionit për një reagim sa më të shpejtë dhe efikas ndaj incidenteve apo sulmeve kibernetike.

Një strukturë shumë e rëndësishme për zbatimin e masave të Sigurisë Kibernetike janë Operatorët e infrastrukturës kritike të informacionit, të cilët sipas përkufizimit në nenin 5, pika 21 është çdo person fizik ose juridik, që administron infrastrukturën kritike të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj.
Neni 12, në pikën 2, përcakton se: identifikimi i operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, sipas përcaktimeve të bëra në anekset I dhe II të këtij ligji, kryhet mbi bazën e një metodologjie, e cila miratohet me vendim të Këshillit të Ministrave.

Në kushtet kur metodologjia për identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishëm ende nuk është miratuar, identifikimi më i fundit ligjor që përcakton Operatorin Administrues është VKM nr. 553, datë 15.7.2020, të Këshillit të Ministrave, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe listës së infrastrukturave të rëndësishme të informacionit", ndryshuar me VKM nr.761, datë 12.12.2022.
Pra, bazuar në këtë vendim, DPT është Operatori Administrues i infrastrukturës kritike e-Taxation, ku përcaktohet se:

- Në pikën 3: Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të zbatojnë të paktën nivelet minimale të kërkesave të sigurisë së informacionit, të miratuara nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike;
- Shtojca nr.2: Infrastruktura e-Taxation nuk është klasifikuar si kritike, por si e rëndësishme;
- Shtojca nr.2: Operatori Administrues për sistemin e-Taxation është Drejtoria e Përgjithshme e Tatimeve.

Riklasifikimi i infrastrukturës e-Taxation në listën kritike është rekomanduar nga KLSH me Raportin Përfundimtar dhe Rekomandimet për auditimin e sistemeve të teknologjisë së informacionit, përcjellë në Drejtorinë e Përgjithshme të Tatimeve në vitin 2023, me shkresën nr.359/8 prot, datë 15.09.2023, për të cilin AKSHI ka marrë masat e nevojshme për të propozuar ndryshimet ligjore në Shtojcën 1 të VKM nr.761, datë 12.12.2022 "Për disa shtesa dhe ndryshime në vendimin nr.553, datë 15.7.2020, të Këshillit të Ministrave, ku sistemi e-Taxation nga një sistem i rëndësishëm në Shtojcën 2, të kategorizohet si një sistem kritik në Shtojcën 1. Ky ndryshim pritet të pasqyrohet dhe të miratohet në vijim në përditësimet e këtyre listave nga Autoriteti përgjegjës për Sigurinë Kibernetike.

Operatorët e infrastrukturave kritike kanë detyrime shumë të rëndësishme në zbatimin e Ligjit nr.25/2024 "Për Sigurinë Kibernetike", në disa prej neneve të tij që janë:

- Neni 17 "Detyrat e CSIRT-it pranë operatorëve të infrastrukturave kritike të informacionit dhe të rëndësishme të informacionit";
- Neni 18 "Pikat e kontaktit";
- Neni 19 "Shkëmbimi i informacionit"
- Neni 20 "Masat e sigurisë kibernetike";
- Neni 21 "Masat për menaxhimin e riskut për operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit";
- Neni 22 "Masat e sigurisë kibernetike në rast kërcënimi ose incidenti të sigurisë kibernetike";
- Neni 23 "Rreziqet e sigurisë kibernetike dhe raportimi i incidenteve të sigurisë kibernetike";
- Neni 24 "Masat shtesë të sigurisë kibernetike";
- Neni 25 "Njoftimi vullnetar i incidenteve të sigurisë kibernetike";
- Neni 26 "Informimi i publikut dhe i përdoruesve për incidentet kibernetike";
- Neni 31 "Detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit".

Detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit janë cilësuar në nenin 31, në të cilat renditen:

- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë të gjitha infrastrukturat e tyre kritike, të rëndësishme, si dhe të gjitha infrastrukturat e tjera që ndërveprojnë me to pranë Autoritetit.
- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë pranë Autoritetit në vazhdimësi çdo infrastrukturë të re, të administruar prej tyre, që ndërvepron me infrastrukturat e kategorizuara kritike apo të rëndësishme.

- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të dokumentojnë çdo ndryshim dhe zhvillim të kryer në infrastrukturat e tyre kritike dhe të rëndësishme.
- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të vendosin në dispozicion të Autoritetit çdo dokumentacion dhe evidencë që kërkohet nga Autoriteti në kuadër të procesit të kontrollit.
- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në kuadër të aktivitetit mbikëqyrës, i ofrojnë CSIRT-së Kombëtar akses të drejtpërdrejtë në ambientet dhe sistemet e tyre të informacionit, në zbatim të procedurave të sigurisë të çdo operatori të këtyre infrastrukturave, të cilat janë të lidhura me shërbimet e ofruara prej tyre.
- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të zbatojnë masat korrigjuese të lëna nga Autoriteti, si dhe të raportojnë për zbatimin e tyre.
- Për implementimin efektiv të masave të sigurisë kibernetike, operatorët paraqesin pranë Autoritetit raportin e vlerësimit të konformitetit nga një organ i vlerësimit të konformitetit për sigurinë kibernetike të paktën një herë në 2 vjet.
- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të marrin masa të shtuara teknike, në përputhje me përcaktimet e bëra në vendimin e Këshillit të Ministrave, për përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë kibernetike.
- Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të bashkëpunojnë me Autoritetin në kuadër të realizimit të funksioneve mbikëqyrëse, të përcaktuara në këtë ligj.

Ligji nr. 43/2023, datë 15.06.2023, "Për qeverisjen elektronike".

Detyrat e AKSHI-t si ofrues shërbimesh dhe si krijues, zhvillues dhe administrues i sistemeve dhe infrastrukturave përcaktohen në nenet 25 dhe 26 të këtij ligji. Ndër detyrat e këtij institucioni, ato që lidhen me objektin e auditimit Siguria Kibernetike për infrastrukturën kritike e-Taxation, janë:

- Neni 25 "Detyrat e AKSHI-t si ofrues shërbimesh", pika dh ku citohet se "*Garanton implementimin e masave të sigurisë kibernetike për të gjitha infrastrukturat kritike të informacionit në cilësinë e operatorit qeveritar që menaxhon këto infrastruktura*".
- Neni 26 "Detyrat e AKSHI-t si krijues, zhvillues dhe administrues i sistemeve dhe i infrastrukturave", pika c ku citohet se "*Administron nga ana teknike çdo sistem TIK, që ka si përdorues institucionet apo organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave në përputhje me këtë ligj. Regjistrat e të dhënave të këtyre institucioneve, që përbëhen nga bazat e të dhënave, mbeten në administrimin e institucioneve respektive*".

Në Agjencinë Kombëtare të Shoqërisë së Informacionit është ngritur struktura qeveritare CSIRT sektorial qeveritar, e cila garanton implementimin e masave të sigurisë kibernetike për të gjitha infrastrukturat kritike të informacionit në cilësinë e operatorit qeveritar që menaxhon këto infrastruktura, ku bën pjesë dhe sistemi e-Taxation. Kjo strukturë bazohet në ligjin nr. 25/2024, "Për Sigurinë Kibernetike", neni 5, pika 6, që përkufizon se: "CSIRT qeveritar" është CSIRT-i sektorial, i cili menaxhon të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit për sektorin qeveritar.

Po në këtë ligj përcaktohen detyrimet **e** *Operatorit Administrues*, që për infrastrukturën e-Taxation është Drejtoria e Përgjithshme e Tatimeve, përcaktuar në VKM nr.761, datë 12.12.2022 "Për disa shtesa dhe ndryshime mbi vendimin nr.553, datë 15.7.2020, të Këshillit të Ministrave, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe listës së infrastrukturave të rëndësishme të informacionit".

Drejtoria e Përgjithshme e Tatimeve, që prej vitit 2018 nuk ka në strukturën e saj asnjë punonjës të TIK, pas transferimit tek AKSHI që u bazua në VKM nr.673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit" i ndryshuar.

Gjithashtu, DPT ka transferuar asetet e TIK-së tek AKSHI, një proces i cili ka përfunduar në fund të vitit 2022, në të cilin janë përfshirë jo vetëm pajisjet fizike servera, router etj, por dhe sistemet informatike që janë ndërtuar dhe janë funksionalë aktualisht.

Strategjia Kombëtare për Sigurinë Kibernetike[1].
Për miratimin e Strategjinë Kombëtare për Sigurinë Kibernetike dhe planit të veprimit 2020-2025, ngarkohet Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, ministritë e institucionet e tjera përgjegjëse të përcaktuara në këtë strategji si dhe në planin e veprimit.
Në drejtim të infrastrukturave kritike, Strategjia Kombëtare i referohet Politikës 1 dhe objektivave specifik për realizimin e saj, si më poshtë:
Qëllimi i politikës 1: Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike. Objektivat specifikë të kësaj politike janë si më poshtë:
Objektivi specifik 1: Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i i tij me direktivat dhe rregulloret e Bashkimit Evropian.
Objektivi specifik 2: Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar.
Objektivi specifik 3: Fuqizimi dhe implementimi i masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit.
Objektivi specifik 4: Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm.

Gjithashtu, në pikën 2.1.1 të Strategjisë Kombëtare, për sigurinë kibernetike në infrastrukturat kritike të informacionit, citohet se "Në infrastrukturat qeveritare kritike të informacionit që përdoren nga institucionet publike, përkatësisht të alokuara pranë qendrës së të dhënave qeveritare, dhe që menaxhohen nga Agjencia Kombëtare e Shoqërisë së Informacionit, aplikohen të gjitha masat e sigurisë konform legjislacionit në fuqi dhe standardit ISO 27001.
AKSHI është CSIRT sektorial qeveritar dhe është certifikuar me këtë standard në vitin 2018 dhe mbi çdo infrastrukturë qeveritare nën administrim të AKSHI-t, aplikohen politikat e standardit ISO 27001.
Plani i Veprimit i Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, është rishikuar për periudhën 2024-2025. Ndërmjet të tjerash, me Planin e Veprimit 2024-2025 kërkohet të arrihen rezultatet e mëposhtme të synuara edhe nga Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025:
- Përmirësimi i kornizës politike dhe ligjore, duke përfshirë ligjet, politikat strategjike, rregulloret, metodologjitë dhe procedurat, përmes implementimit të politikave dhe standardeve të sigurisë kibernetike të BE-së gjithashtu.
- Fuqizimi i strukturave dhe infrastrukturave të sigurisë kibernetike sa i përket kapaciteteve teknike dhe profesionale si dhe procedurave e tyre përkatëse. Kjo planifikohet të arrihet përmes aktiviteteve të tilla si: përmirësimi i kapaciteteve të Qendrës Kombëtare Operacionale të Sigurisë Kibernetike (SOC) për monitorimin dhe trajtimin e incidenteve të sigurisë kibernetike, ngritja e laboratorëve të analizave të programeve me qëllim të keq (malware), hetimit kibernetik dhe simulimit të incidenteve kibernetike, rritja e kapaciteteve teknike dhe profesionale, analiza teknologjike të mjedisit të infrastrukturave kritike, optimizimi i infrastrukturës së sigurisë, përmirësimi i procedurave të trajtimit dhe menaxhimit të incidenteve dhe të tjera, të cilat parashikohen në planin e veprimit.

Rregullorja mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit, në versionin më të fundit 3.0, miratuar nga titullari i

[1] VKM nr. 1084, datë 24.12.2020, "Për miratimin e Strategjinë Kombëtare për Sigurinë Kibernetike dhe planit të veprimit 2020-2025"

AKSK[2], është hartuar në zbatim të ligjit nr. 2/2017, "Për Sigurinë Kibernetike", Vendimit të Këshillit të Ministrave nr. 141, datë 22.2.2017, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike" si dhe Vendimit të Këshillit të Ministrave nr.553, datë 15.07.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit"e ndryshuar.
Qëllimi i kësaj rregulloreje është arritja e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike, në përmbushje të detyrave specifike do të kontrollojë infrastrukturat kritike te rëndësishme te informacionit.

1. Gjetje nga auditimi: Megjithëse, Drejtoria e Përgjithshme e Tatimeve është përcaktuar si Operator Administrues për sistemin kritik e-Taxation, sipas VKM nr. 553, datë 15.7.2020, e ndryshuar me VKM nr. 761, datë 12.12.2022, infrastruktura e këtij sistemi administrohet nga AKSHI. Ndërkohë, mungon ende një metodologji e miratuar për identifikimin dhe kategorizimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, siç parashikohet në nenin 12, pika 2, të ligjit nr. 25/2024 "Për Sigurinë Kibernetike".

2. Gjetje nga auditimi: Rregullorja e miratuar nga Autoriteti Kombëtar i Sigurisë Kibernetike me urdhrin nr. 97, datë 05.03.2024, mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit (v3.0) përcakton që Drejtoria e Përgjithshme e Tatimeve është Operatori Administrues për sistemin e-Taxation dhe ka detyrimin për dokumentimin dhe zbatimin e masave të Sigurisë Kibernetike. Kjo rregullore është në mospërputhje me nenin 25 të Ligjit nr. 43/2023, datë 15.06.2023, i cili përcakton se Autoriteti Kombëtar i Sigurisë Kibernetike është përgjegjës për implementimin e masave të sigurisë kibernetike për të gjitha infrastrukturat kritike të informacionit, duke vepruar si operator qeveritar që menaxhon këto infrastruktura.

3. Gjetje nga auditimi: Drejtoria e Përgjithshme e Tatimeve nuk disponon mekanizmat ligjorë dhe teknikë të nevojshëm për të menaxhuar efektivisht regjistrat e të dhënave, sikurse përcaktohet në nenin 26 të Ligjit nr. 43/2023, datë 15.06.2023 "Për qeverisjen elektronike", duke përfshirë mbajtjen dhe ruajtjen e të dhënave të ndjeshme dhe kritike.

1.Konkluzion: Auditimi identifikoi mangësi ligjore, që janë: mungesa e një metodologjie për identifikimin dhe kategorizimin e operatorëve të infrastrukturave kritike, mospërputhje midis rregullores për dokumentimin dhe implementimin e masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit dhe ligjit për qeverisjen elektronike, si dhe mungesën e mekanizmave ligjorë dhe teknikë të nevojshëm për menaxhimin efektiv të regjistrave të të dhënave nga Drejtoria e Përgjithshme e Tatimeve.

1.1 Rekomandim: Autoriteti Kombëtar për Sigurinë Kibernetike, të hartojë metodologjinë mbi identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, në të cilën Agjencia Kombëtare e Shoqërisë së Informacionit të përfshihet si operator bashkëpërgjegjës për infrastrukturat kritike të cilat janë qendërzuar. Mbështetur në metodologjinë për identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, të hartohen propozimet për ndryshimet ligjore të nevojshme të Vendimit të fundit të Këshillit të Ministrave me nr.761, datë 12.12.2022.

Brenda vitit 2025

[2] Urdhri nr. 97 datë 05.03.2024

2.1 Rekomandim: Autoriteti Kombëtar për Sigurinë Kibernetike të përmirësojë rregulloren mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe të hartojë një mënyrë bashkëpunimi dhe komunikimi ndërmjet tyre, e cila do të ndihmojë institucionet të angazhohen dhe të veprojnë sipas përgjegjësisë në drejtim të sigurisë kibernetike.

Brenda vitit 2025

3.1 Rekomandim: Autoriteti Kombëtar i Sigurisë Kibernetike, në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit dhe Drejtorinë e Përgjithshme të Tatimeve, të ndërmarrin nisma për ndryshime ligjore dhe rregullatore, me qëllim përcaktimin e qartë të rolit dhe përgjegjësive të Drejtorisë së Përgjithshme të Tatimeve për menaxhimin e regjistrave të të dhënave, duke siguruar mbrojtjen efektive ndaj kërcënimeve kibernetike.

Brenda vitit 2025

4.2 A janë ndërmarrë masa organizative, për parandalimin, mbrojtjen ndaj cenimeve kibernetike?

AKSHI ka përmbushur politikat e sigurisë kibernetike dhe ka hartuar strategjinë e backup të çdo sistemi dhe elementi tjetër të ambientit teknologjik, sipas kërkesave të legjislacionin shqiptar në fuqi dhe të udhëzimeve dhe praktikave me të mira ndërkombëtare.

Me VKM nr.710, datë 21.08.2013[3], përcaktohen masat që duhen marrë për të garantuar Agjencinë Kombëtare të Shoqërisë së Informacionit dhe institucionet e tjera publike që të mbrojnë dhe ruajnë në mënyrë të sigurt bazat e të dhënave, sistemet, aplikacionet dhe elementët e tjerë të ambientit teknologjik që ato menaxhojnë dhe administrojnë. Këto masa mundësojnë ruajtjen e të dhënave në më tepër sesa një kopje për periudha kohore që janë në përpjesëtim me rëndësinë e elementeve që po ruhen.

Po kështu, masat lidhen drejtpërdrejt me përgatitjen për të garantuar në mënyrë të pandërprerë dhe me disponueshmëri të lartë operacionet e punës dhe ofrimin e shërbimeve për qytetarët, bizneset dhe institucionet e administratës shtetërore si dhe për të rikthyer në gjendje normale funksionale pune sistemet dhe shërbimet në raste të incidenteve që vijnë si pasojë e "fatkeqësive".

Për të gjithë elementet e përmendur më sipër do të duhet të implementohen strategji të backup-it për të minimizuar sa më tepër ndërprerjen e operacioneve dhe për të rikuperuar vazhdimësinë e punës sa më shpejt që të jetë e mundur në rast të paraqitjes së një incidenti apo fatkeqësie.

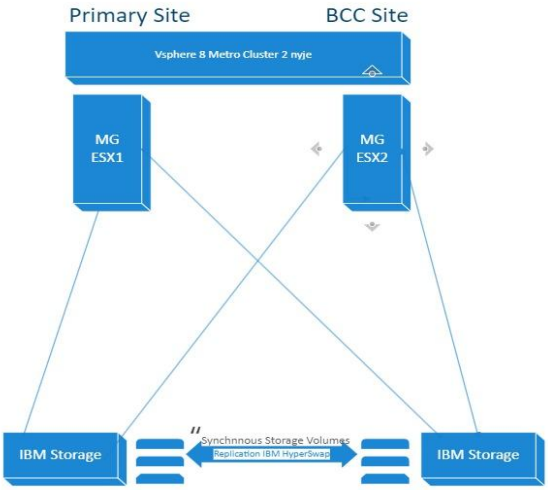
Ndërsa AKSHI në përmbushje të politikave, harton strategjinë e backup për çdo sistem ose element tjetër të ambientit teknologjik duke zbatuar legjislacionin shqiptar në fuqi dhe udhëzimet e praktikave me të mira ndërkombëtare.

Evidentohet se, megjithëse AKSHI ka hartuar strategji për backup, por distanca ndërmjet *primary site dhe sekondar,* nuk plotëson largësinë e duhur mbështetur nga praktikat me të mira të fushës dhe në udhëzimin për zbatimin e dokumentit të përditësuar të politikave të vazhdimësisë së punës dhe planit për ruajtjen e informacionit[4]. Më poshtë në figurën 5 paraqitet skema infrastrukturore *parësore* dhe dytësore, ndërtuar për ofrimin e vazhdimësisë së punës dhe shërbimit pa ndërprerje.

3 VKM nr.710, datë 21.08.20133 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar.

[4] Udhëzimi i Agjencisë Kombëtare Të Shoqërisë së informacionit Nr.1, datë 30.07.2023 "Për zbatimin e Dokumentit të përditësuar të politikave të vazhdimësisë së pumës dhe planit për ruajtjen e informacionit"[4]

Figura 5: Skema logjike e infrastrukturës së BCC Site



Masat e marra për ngritjen e një mjedisi të sigurt me personel dhe me edukimin e duhur për sigurinë kibernetike.

Zhvillimi i trajnimeve ka një rëndësi të veçantë për menaxhimin e kapaciteteve njerëzore në institucion. Punonjësit të cilët kanë akses në sistemet e informacionit duhet të jenë të njohur me standardet e sigurisë dhe të gëzojnë aftësinë për zbatimin dhe implementimin e tyre gjatë aktivitetit që kryejnë. Është e nevojshme që të identifikohen nevojat e stafit për trajnime mbi teknologjinë e informacionit dhe sigurinë kibernetike.
Në lidhje me trajnimet e personelit, rregullorja për sigurinë e informacionit[5] ka përcaktuar se, personat që kanë akses në asetet e informacionit të institucionit përfitues janë të detyruar të jenë të vetëdijshëm për rregullat dhe standardet e sigurisë në institucionin përfitues. I gjithë personeli duhet të marrë trajnimin e nevojshëm për rregullat dhe për procedurat organizative dhe të sigurisë. Nevojat për trajnim përcaktohen menjëherë nga Drejtori i Drejtorisë, i cili ja përcjell zyrtarisht kërkesën Drejtorisë së Burimeve Njerëzore.
Po kështu kjo rregullore ka përcaktuar edhe objektivat e Trajnimit në lidhje me sigurinë të cilat janë:

- krijimi i kulturës së sigurisë në të gjithë institucionet përfitues;
- edukimi i personelit mbi pasojat e veprimeve të tyre mbi sigurinë e informacionit;
- udhëzimi i personelit për rregullat dhe procedurat e sigurisë sipas pozicioneve përkatëse;
- përcaktimi i përgjegjësive që mban çdo person mbi sigurinë dhe detyra e secilit për të raportuar çdo shkelje të rregullave të sigurisë.

Gjithashtu edhe rregullorja për mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit[6], ka përcaktuar se, AKSHI duhet të implementojë programe trajnimi, për të siguruar që personeli të ketë njohuri të mjaftueshme dhe të përditësuara për sigurinë kibernetike sipas profilit të punës, si dhe duhet të informojë dhe trajnojë personelin e ri mbi politikat dhe procedurat në fuqi.

Evidentohet se, për periudhën objekt auditimi nuk janë planifikuar dhe realizuar trajnime për të gjithë personelin e nevojshëm për rregullat dhe për procedurat organizative dhe të sigurisë nga vetë AKSHI, por janë kryer vetëm trajnime me tema lidhur me sigurinë kibernetike me ftesë për pjesëmarrje të organizuara nga AKSK.

[5] Rregullore Nr. 2 Datë 06.11. .2023 "Për sigurinë e informacionit", miratuar me Urdhër të Drejtorit të AKSHI-t
[6] Pika 1.5, gërma b dhe c e Rregullore mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit, miratuar me Urdhrin Nr. 97 datë 05.03.2024

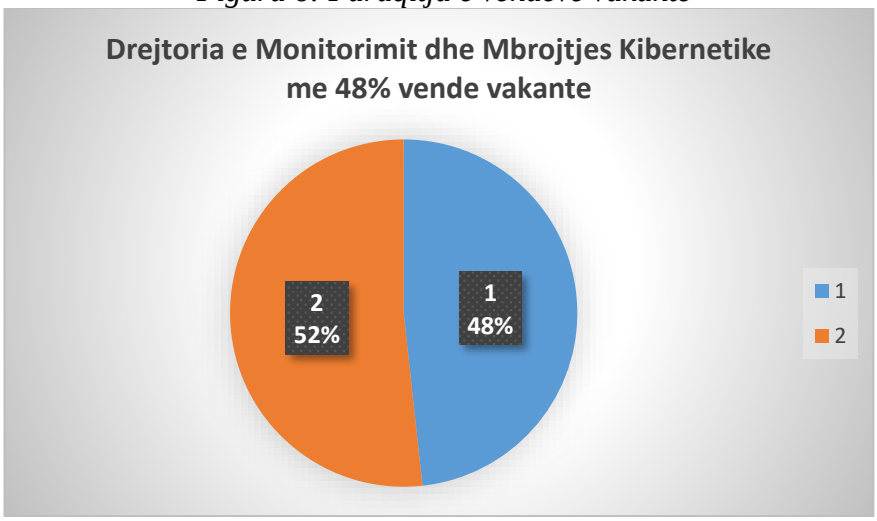
AKSHI nuk ka marrë masa për të plotësuar strukturën organizative të sigurisë kibernetike

Me urdhër të Kryeministrit nr.13, datë 25.01.2024 është miratuar struktura e Agjencisë Kombëtare të Shoqërisë së Informacionit dhe Rregullorja e Brendshme[7] mbi Detyrat dhe Funksionimin e AKSHI-t nr.1900 prot, datë 16.04.2020. Në këtë strukturë brenda AKSHI-t është ngritur dhe funksionon Drejtoria e Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-Gov. Në rregulloren e brendshme për funksionimin e AKSHI-t janë përcaktuar hollësisht edhe përshkrimet e punës të secilit pozicion të organikës së kësaj drejtorie. Përgjithësisht kjo drejtori kryen këto detyra:

- monitoron eventet e sigurisë të detektuara nga SIEM ose platformat e tjera të sigurisë;
- siguron zbatimin e legjislacionit në fuqi për ruajtjen e të dhënave personale;
- analizon emailet phishing dhe incidente të tjera të eskaluara nga përdoruesit fundor.
- kryen hetimin fillestar të alerteve ose incidenteve kibernetike;
- merr masat përkatëse ndaj incidenteve kibernetike jo-komplekse të nivelit të ulët në proporcion me Manualin e Reagimit ndaj Incidenteve Kibernetike;
- dokumenton alertet e detektuara dhe masat e marra në raport ditor;
- raporton tek eprori për rastet e mosrespektimit të standardeve të sigurisë dhe propozon masa për rregullimin e situatës;
- merr pjesë në trajnimet periodike që do të zhvillohen nga Microsoft për rritjen e kapaciteteve teknike;
- analizon, implementon sistemet e sigurisë së informacionit;
- analizon loget e nxjerra periodikisht nga sistemet e monitorimit dhe realizon raporte.

Drejtoria e Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-Gov që është brenda strukturës organizative të AKSHIT-t (TIK), ka në përbërje, Sektorin e Qendrës Operacionale të Sigurisë, Sektorin e Sigurisë dhe Konformitetit, Sektori i Reagimit ndaj Incidenteve të Sigurisë, Sektori i Infrastrukturës së Çelësave Publikë me 29 punonjës gjithsej të miratuar në organikë. Evidentohet se nga 29 punonjës të miratuar në organikë ky sektorë është plotësuar vetëm me 15 punonjës dhe 14 vende pune të tjera janë të pa plotësuara ose është e pa plotësuar 48% e organikës.

Figura 6: Paraqitja e vendeve vakante



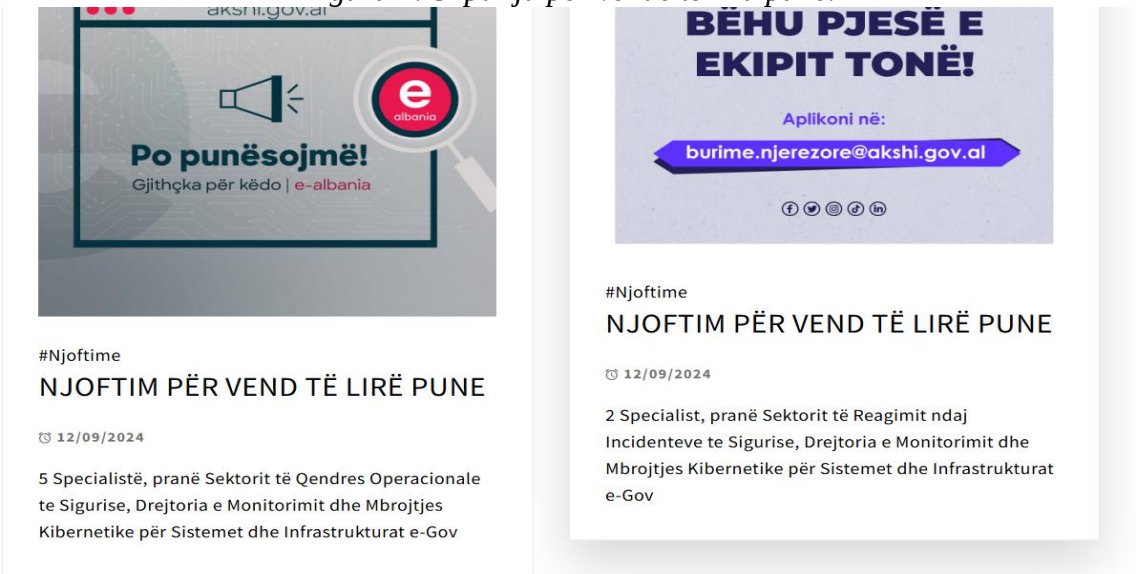
Punoi:Grupi i auditimit

Përveë kësaj Drejtorie, në strukturën dhe organikën e AKSHI-t, është atashuar pranë DPT edhe Drejtoria Teknologjinë e Informacionit dhe Komunikimit (TIK) me organikë 41 punonjës gjithsej. Në përbërje të kësaj Drejtorie përfshihet edhe Sektori i Sigurisë të të dhënave me organikë 3 punonjës, por ky sektor është i pa plotësuar me këtë personel.

[7] Mbi Detyrat dhe Funksionimin e AKSHI-t Nr.1900 prot…datë 16.04.2020

Megjithëse, gjatë periudhës objekt auditimi, për plotësimin e vendeve vakantë, në zbatim, të strukturës të miratuar me urdhër të Kryeministrit nr.13, datë 25.01.2024, dhe akteve ligjore e nënligjore që rregullojnë fushën e punësimit, AKSHI ka shpallur dhe ka publikuar njoftimet për konkurimin në pozicionet vakante kryesisht për Drejtorinë e Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-Gov si dhe për Sektorin e Qendrës Operacionale dhe Sektorin e Reagimit ndaj Incidenteve. Po përsëri këto vakanca deri në periudhën e ushtrimit të këtij auditimi nuk janë plotësuar tërësisht sipas strukturës dhe organikës të miratuar.

Figura 7: Shpallja për vende të lira pune.



4. Gjetje nga auditimi: Referuar kërkesave specifike të përcaktuara në udhëzimin nr.1, datë 30.07.2023 të Agjencisë Kombëtare të Shoqërisë së Informacionit, nuk është respektuar distanca e duhur e vendndodhjeve ndërmjet *primary site* dhe *secondary site*. Në këto dokumente përcaktohet që vendndodhja dytësore do të jetë gjithmonë në një pozicion gjeografik që ka risk shumë të ulët me qëllim mos përfshirjen nga i njëjti incident apo fatkeqësi natyrore nga ambienti primar dhe sipas kushteve teknike kërkohet minimalisht një distancë prej 50 km në vijë ajrore. Kjo distancë duhet të jetë e mjaftueshme për të siguruar që të dyja lokacionet nuk janë të prekshme nga i njëjti incident (fatkeqësi natyrore: tërmete, zjarre, përmbytje etj.).

5. Gjetje nga auditimi: Për periudhën e audituar, Agjencia Kombëtare e Shoqërisë së Informacionit nuk ka dokumentuar plane, propozime apo kërkesa për zhvillimin e trajnimeve, që do të plotësonin nevojat për njohuri të zgjeruara mbi sigurinë kibernetike. Gjithashtu, institucioni nuk disponon një plan për trajnimin e përdoruesve fundorë, jo vetëm si një element i rëndësishëm në rritjen profesionale të punonjësve, por dhe minimizimin e rreziqeve të brendshme.

6. Gjetje nga auditimi: Drejtoria e Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-Gov, e vendosur pranë Agjencisë Kombëtare të Shoqërisë së Informacionit, është e pa plotësuar me personel dhe funksionon aktualisht me vetëm 15 punonjës nga 29 që parashikohen në organikë. Po ashtu, pranë Drejtorisë së Përgjithshme të Tatimeve, struktura e atashuar TIK e Agjencisë Kombëtare të Shoqërisë së Informacionit ka një organikë të miratuar me 41 punonjës, përfshirë Sektorin e Sigurisë së të Dhënave me 3 pozita të miratuara. Megjithatë, ky sektor është plotësisht i pa plotësuar dhe të gjitha pozitat janë vakante.

***2.Konkluzion*:** Auditimi evidentoi disa mangësi, ku përfshihen mosrespektimi i distancës minimale ndërmjet primary site dhe secondary site, mungesa e dokumentacionit për trajnime mbi sigurinë

kibernetike dhe trajnimin e përdoruesve fundorë, si dhe vendet e paplotësuar me personel në Drejtorinë e Monitorimit dhe Mbrojtjes Kibernetike dhe sektorin e Sigurisë së të Dhënave.

4.1 Rekomandim: Agjencia Kombëtare e Shoqërisë së Informacionit duhet të marrë masa për të siguruar që vendndodhja e *secondary site* të jetë gjithmonë në një pozicion gjeografik që ndodhet minimalisht 50 km larg nga *primary site* në vijë ajrore. Kjo është një masë e rëndësishme për të garantuar disponueshmërinë dhe vazhdimësinë e shërbimeve në rast të një ngjarjeje të papritur apo katastrofike që mund të prekte *primary site*. Vendosja e *secondary site* në një distancë të tillë do të ndihmojë në ruajtjen dhe disponueshmërinë e të dhënave, ndaj fatkeqësive natyrore që mund të ndodhin në një zonë të caktuar.

Në vijimësi

5.1 Rekomandim: Agjencia Kombëtare e Shoqërisë së Informacionit duhet të zhvillojë dhe dokumentojë një plan të detajuar për trajnimin e punonjësve, duke përfshirë një program të strukturuar për trajnimet mbi sigurinë kibernetike dhe teknologjinë e informacionit. Ky plan duhet të përfshijë analiza të nevojave për trajnim dhe propozime për zhvillimin e kurseve të specializuara që përmirësojnë aftësitë e punonjësve dhe ndihmojnë në minimizimin e rreziqeve të brendshme. Po ashtu, duhet të krijohet një program trajnimi për përdoruesit fundorë që përfshin praktikat më të mira për mbrojtjen e informacionit dhe sigurinë kibernetike, duke kontribuar në rritjen e ndërgjegjësimit dhe përgatitjen e tyre për menaxhimin e rreziqeve kibernetike.

Menjëherë në vijimësi

6.1 Rekomandim: Agjencia Kombëtare e Shoqërisë së Informacionit, të marrë masa për plotësimin e vendeve vakante në strukturën e Teknologjisë së Informacionit dhe Komunikimit të miratuar për Drejtorinë e Përgjithshme të Tatimeve dhe në Drejtorinë e Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-Gov.

Brenda vitit 2025

4.3 A janë ndërmarrë masa teknike, për parandalimin, mbrojtjen dhe reagimin për sigurinë kibernetike?

AKSHI si institucion publik qendror në varësi të Kryeministrit, në veprimtarinë e tij në bazë të Ligjit nr. 43/2023 "Për Qeverisjen Elektronike" dhe VKM-së nr. 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit, i ndryshuar ka për mision të:
- administrojë çdo sistem TIK që ka si përdorues institucionet apo organet e administratës shtetërore nen përgjegjësinë e Këshillit te Ministrave;
- garantojë dhe implementojë masat e sigurisë kibernetike për të gjitha infrastrukturat kritike të informacionit në cilësinë e operatorit qeveritar që menaxhon këto infrastruktura;
- garantojë një nivel të lartë të sigurisë kibernetike dhe zgjidhjet ndaj incidenteve të sigurisë kompjuterike duke bashkërenduar me CSIRT, si ekipi përgjegjës ndaj incidenteve të sigurisë kompjuterike, për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave;
- administrojë kodin në burim të çdo sistemi, si përfaqësues i pronarit shtet që është këshilli i ministrave.

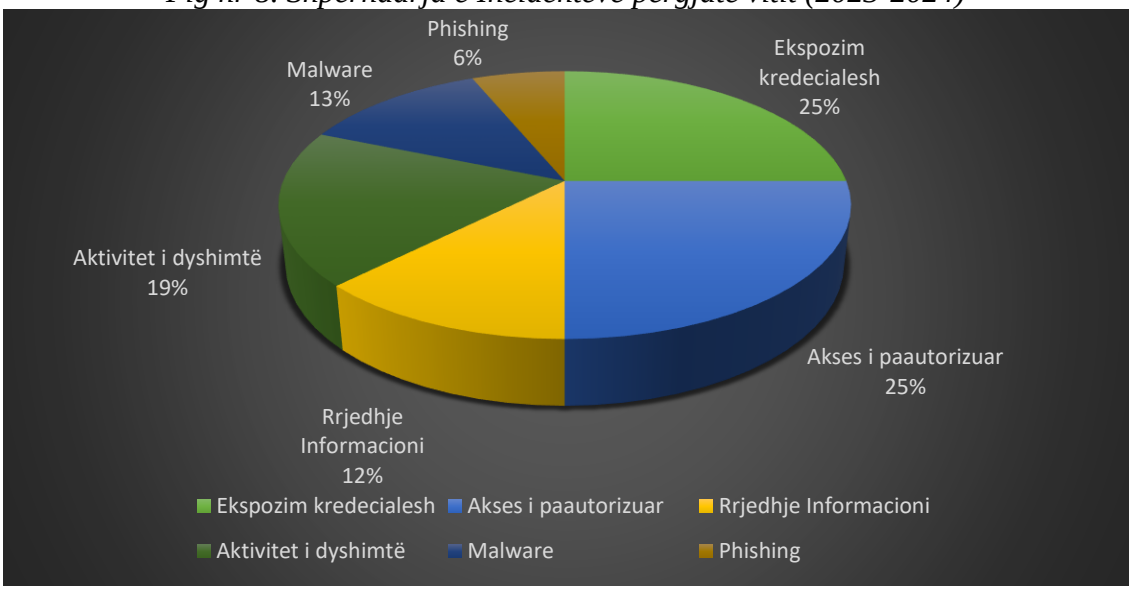
Drejtoria përgjegjëse për sigurinë kibernetike në Agjencinë Kombëtare të Shoqërisë së Informacionit është Drejtoria e Monitorimit dhe Mbrojtjes Kibernetike për sistemet dhe Infrastrukturat e-Gov. Në Drejtorinë e Përgjithshme të Tatimeve ndodhet e atashuar një Strukturë IT e Akshit dhe ka për objektiv:
- krijimimin dhe zhvillimin e të gjithë infrastrukturës së teknologjisë së informacionit dhe komunikimit, lehtësirave, dhe shërbimeve të nevojshme për administratën tatimore dhe

tatimpaguesit, me qëllim realizimin e misionit dhe objektivave të Drejtorisë së Përgjithshme të Tatimeve;
- krijimin e mundësive për përdorimin sa më efikas dhe efektiv të teknologjive të informacionit dhe komunikimit për të rritur bashkëpunimin ekzistues midis njësive organizative të Drejtorisë së Përgjithshme të Tatimeve, Drejtorive Rajonale, si dhe për të nxitur bashkëpunime të reja me institucione të tjera qeveritare dhe jo qeveritare, brenda dhe jashtë vendit;
- krijimin dhe zhvillimin e sistemeve të integruara të informacionit. Drejtoria është e angazhuar për mbarëvajtjen e punës dhe sigurimin e funksionalitetit të të gjithë sistemeve elektronik të DPT, ku nder sistemet me te rëndësishëm është dhe Sistemi e-TAX (C@TS & eFiling).

Incidentet Kibernetike të regjistruara në DPT nga AKSHI (Periudha 2023-2024)

Incidentet që lidhen me sigurinë janë të paevitueshme në çdo institucion, por aftësia për t'i vlerësuar dhe për të reaguar në mënyrë efikase përcakton qëndrueshmërinë e përgjithshme të sistemit. Gjatë rishikimit të incidenteve të raportuara nga AKSHI për Drejtorinë e Përgjithshme të Tatimeve gjatë vitit 2023 dhe 2024, janë identifikuar gjithsej 21 raste, duke nxjerrë në pah sfida të ndryshme të përsëritura në ruajtjen e integritetit të sistemit dhe mbrojtjen e të dhënave. Incidentet e listuara që kanë ndodhur, janë lokalizuar në kohë dhe nuk kanë shkaktuar dëme me impakt të lartë.
Një nga çështjet më të rëndësishme të vërejtura është ekspozimi ose kompromisi i kredencialeve të përdoruesit. Incidente të tilla si ekspozimi i kredencialeve dhe rivendosjet e paautorizuara nxjerrin në pah nevojën për mekanizma më të fortë vërtetimi. Për më tepër, politikat e fjalëkalimeve duhet të zbatojnë kompleksitetin dhe përditësimet e rregullta dhe duhet të futen mjete të sigurta të menaxhimit të fjalëkalimeve, për të zbutur kërcënimet.

Fig nr 8. Shpërndarja e Incidenteve përgjatë vitit (2023-2024)



Burimi AKSHI. Përpunuar nga grupi i KLSH.

Ekspozimi dhe Keqpërdorimi i Kredencialeve

Incidentet tregojnë se kredencialet e privilegjuara dhe standarde të përdoruesve janë ekspozuar ose keqpërdorur, duke çuar në shkelje të mundshme të sigurisë. Rastet që përfshijnë përdorimin e kredencialeve të administratorit në kontekste të paautorizuara dhe rrjedhje individuale të kredencialeve sugjerojnë se kontrollet e aksesit mund të mos zbatohen siç duhet, duke i bërë sistemet kritike të prekshme. Kur kredencialet ekspozohen, sulmuesit mund t'i shfrytëzojnë ato për të fituar akses të paautorizuar, për të përshkallëzuar privilegjet ose për të nisur sulme të mëtejshme kibernetike. Këto tregojnë mungesë të mekanizmave të sigurt të vërtetimit dhe monitorim të

pamjaftueshëm të aktivitetit të kredencialeve, duke rritur rrezikun e kërcënimeve të brendshme dhe shkeljeve të jashtme.

- Probleme me aksesin dhe hyrjen e paautorizuar

Disa anomali identifikimi tregojnë se kanë ndodhur përpjekje të paautorizuara për të hyrë në sistem. Këto incidente ngrenë shqetësime në lidhje me sigurinë e vërtetimit të përdoruesit, pasi ato mund të tregojnë llogari të kompromet uara ose sulmues që përdorin kredencialet e vjedhura për të depërtuar në sisteme. Pa mekanizma të qartë zbulimi dhe reagimi, aksesi i paautorizuar mund të kalojë pa u vënë re, duke lejuar sulmuesit kibernetikë ose personat e brendshëm me qëllim të keq të shfrytëzojnë informacionet e sistemeve. Për më tepër, dukuritë e përsëritura të anomalive të hyrjes tregojnë se kontrollet parandaluese të sigurisë, të tilla si gjeo-kufizimet dhe zbulimi i anomalive, mund të mos optimizohen.

- Rrjedhje e të Dhënave

Janë identifikuar raste të rrjedhjeve të të dhënave, të cilat paraqesin rreziqe serioze për konfidencialitetin dhe përputhshmërinë rregullatore. Ekspozimi i të dhënave qoftë përmes eksfiltrimit të qëllimshëm apo rrjedhjeve të paqëllimshme, mund të ketë pasoja të rënda. Këto incidente nxjerrin në pah boshllëqet e mundshme në kontrollet e aksesit të të dhënave dhe monitorimin e pamjaftueshëm të rrjedhave të informacionit, duke lejuar përdoruesit e paautorizuar të marrin dhe të shpërndajnë të dhëna. Prania e incidenteve brenda kësaj kategorie tregon një dobësi sistematike në zbatimin e politikave të sigurisë rreth mbrojtjes së të dhënave.

- Aktivitetet e dyshimta

Treguesit e aktivitetit me qëllim të keq, të tillë si sulmet ndaj fjalëkalimit dhe sjelljet e dyshimta të skedarëve, tregojnë një pamje aktive kërcënimi brenda mjedisit të IT-së së Institucionit. Këto incidente tregojnë për sulme të jashtme që synojnë të shkelin mbrojtjen e sigurisë, si dhe gabime të mundshme të sigurisë së brendshme që mund t'u mundësojnë sulmuesve të shfrytëzojnë dobësitë. Zbulimi i përdorimit të paautorizuar të kredencialeve dhe infeksioneve të mundshme malware tregon se sulmuesit mund të hetojnë rrjetin për dobësi. Për më tepër, shfaqja e rasteve të shumta brenda një afati të shkurtër kohor ngre shqetësime në lidhje me efektivitetin e monitorimit të sigurisë dhe aftësive të reagimit ndaj incidenteve.

- Sulmet Malware

Prania e incidenteve të lidhura me malware, duke përfshirë një infektim të mundshëm Raspberry Robin Worm dhe përdorimin e paautorizuar të softuerit peer-to-peer, ngre shqetësime për sigurinë e pikës fundore. Softueri mund të jetë një portë për sulmet e ransomware, korruptimin e të dhënave ose aksesin e vazhdueshëm për aktorët e kërcënimit. Për më tepër, përdorimi i një softueri të palejuar mund të krijojë pika të dobëta sigurie, duke e bërë më të lehtë për *malware* që të depërtojnë në sisteme. Këto tregojnë se mund të ketë kontrolle të pamjaftueshme rreth instalimit të softuerit, menaxhimit të patch-it dhe mbrojtjes së pikës fundore, duke i lënë sistemet vulnerabël.

<u>Njoftimet dhe sinjalizimet e përgjithshme</u>

Të dhënat tregojnë se janë gjeneruar njoftime dhe sinjalizime të shumta sigurie, megjithatë përgjigja dhe klasifikimi i këtyre sinjalizimeve mbeten të paqarta. Fakti që punonjësit raportojnë emaile me tregues të mundshëm të *phishing*-ut, tregon se ndërgjegjësimi për sigurinë mund të mos jetë në nivelin optimal. Për më tepër, alarmet e gjeneruara nga sistemi nëpër platforma të shumta tregojnë se mjetet e monitorimit të sigurisë janë të vendosura, por mund të mos përdoren në mënyrë efektive për të zbuluar dhe zbutur kërcënimet në kohë reale.

7. Gjetje nga auditimi: Për periudhën 2023 - 2024, për Drejtorinë e Përgjithshme të Tatimeve janë identifikuar 21 incidente, ku përsëriten raste të ekspozimit të kredencialeve dhe rivendosjeve të paautorizuara, çfarë tregon për mangësi në zbatimin e politikave të fjalëkalimeve. Megjithëse incidentet janë adresuar në kohë dhe nuk kanë shkaktuar pasoja me impakt të lartë, ekziston një rrezik i vazhdueshëm për kompromet imin e integritetit të sistemit dhe sigurisë së të dhënave, veçanërisht nëse nuk merren masa parandaluese dhe përmirësuese të qëndrueshme.

8. Gjetje nga auditimi: *Data Center-i* Qeveritar është i pajisur me një sistem monitorimi aktiv të integruar me Sistemin e Menaxhimit të Ndërtesave (BMS). Ky sistem është konfiguruar për të dërguar njoftime përmes email-it dhe SMS-së në rast incidentesh të mëdha, duke siguruar një nivel mbikëqyrjeje mbi kushtet e funksionimit të objektit. Bazuar në Rregulloren mbi Mënyrën e Dokumentimit të masave të Sigurisë Kibernetike të Autoritetit Kombëtar për Sigurinë Kibernetike u konstatua se ka mungesë dokumentacioni në lidhje me kontrollet specifike mjedisore, veçanërisht lidhur me mbrojtjen nga përmbytjet, alarmet nga zjarri dhe procedurat e rregullta të testimit të tyre, mungesa e të cilave sjell risk në lidhje me aftësinë e institucionit për t'iu përgjigjur me efikasitet urgjencave.

9. Gjetje nga auditimi: Për sistemin e-Taxation të Drejtorisë së Përgjithshme të Tatimeve, nuk janë hartuar dhe zbatuar politika të qarta për enkriptimin e të dhënave, siç kërkohet nga Rregullorja e Autoritetit Kombëtar për Sigurinë Kibernetike, mungesa e të cilave mund të ndikojë në mbrojtjen e duhur e të dhënave brenda këtij sistemi.

10. Gjetje nga auditimi: Agjencia Kombëtare e Shoqërisë së Informacionit nuk ka një skedulim të qartë dhe të dokumentuar për shqyrtimin e logeve të sistemit E-Taxation. Kjo ndikon në identifikimin e aktiviteteve të dyshimta dhe zbulimin e incidenteve, duke vonuar reagimin ndaj kërcënimeve të sigurisë. Menaxhimi efektiv i logeve është thelbësor për sigurinë e informacionit, duke mundësuar gjurmimin e aktiviteteve të përdoruesve dhe zbulimin e anomalive, për të parandaluar ngjarje kritike dhe për të siguruar një përgjigje të shpejtë dhe të efektshme ndaj kërcënimeve.

11. Gjetje nga auditimi: Agjencia Kombëtare e Shoqërisë së Informacionit ka rolin kryesor në zhvillimin e marrëveshjeve, politikave, procedurave dhe standardeve për kontrollin e aksesit, dhe është hartuesi i kontratave të shërbimeve me palët e treta, sipas nenit 9, të Ligjit nr. 43/2023 "Për qeverisjen elektronike", por përgjegjësitë e aksesit të jashtëm dhe kontrollet e palëve të treta në sistemin kritik e-Taxation të Drejtorisë së Përgjithshme të Tatimeve nuk rezultojnë të jenë të qarta dhe të dokumentuara plotësish.

3. Konkluzion: Nga auditimi i sigurisë kibernetike në lidhje me ndërmarrjen e masave të duhura teknike janë identifikuar disa mangësi dhe risqe që mund të ndikojnë në sigurinë e sistemeve dhe infrastrukturës të Agjencisë Kombëtare të Shoqërisë së Informacionit. Në Data Center-in Qeveritar, mungesa e dokumentacionit dhe kontrolleve specifike mjedisore, veçanërisht ato lidhur me mbrojtjen nga përmbytjet dhe alarmet për zjarr, rrit rrezikun e përgjigjeve të pamjaftueshme ndaj urgjencave. Po ashtu, në sistemin e-Taxation të Drejtorisë së Përgjithshme të Tatimeve, mungesa e politikave të enkriptimit të të dhënave dhe e skedulimit të shqyrtimit të logeve paraqet risk për sigurinë e informacionit, duke e lënë sistemin të ekspozuar ndaj aksesit të paautorizuar dhe ngjarjeve të paidentifikuara në kohë. Gjithashtu, mungesa e dokumentimit të aksesit të jashtëm dhe të kontrolleve për palët e treta në sistemin e-Taxation, përbën risk për akses të paautorizuar.

<u>7.1 Rekomandim</u>: Për të reduktuar rrezikun e incidenteve të përsëritura dhe për të garantuar sigurinë afatgjatë të sistemeve dhe të dhënave, Agjencia Kombëtare e Shoqërisë së Informacionit, të përforcojë menaxhimin e kredencialeve përmes politikave të avancuara të fjalëkalimeve, autentifikimit me shumë faktorë, zgjidhjeve të sigurta për menaxhimin e tyre dhe trajnimeve të vazhdueshme për ndërgjegjësimin e përdoruesve.

<u>8.1 Rekomandim</u>: Agjencia Kombëtare e Shoqërisë së Informacionit, të hartojë e miratojë plane masash, rregullore, dokumente teknike, bazuar edhe në praktikat më të mira ndërkombëtare, mbi kontrollet specifike mjedisore, lidhur me mbrojtjen nga përmbytjet, zjarret etj., procedurat e testimit

dhe dokumentimin e tyre, për aftësinë e institucionit për t'iu përgjigjur me efikasitet urgjencave si dhe vlerësimit periodik të sistemeve të sigurisë mjedisore.

Menjëherë

9.1 Rekomandim: Drejtoria e Përgjithshme e Tatimeve në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit, të marrin masa për hartimin dhe implementimin e politikave të qarta për enkriptimin e të dhënave në sistemin e-Taxation, në përputhje me kërkesat e Rregullores së Autoritetit Kombëtar për Sigurinë Kibernetike, për një mbrojtje më të lartë të të dhënave ndaj kërcënimeve të brendshme, sulmeve kibernetike ose ekspozimit aksidental.

Brenda vitit 2025

10.1 Rekomandim: Agjencia Kombëtare e Shoqërisë së Informacionit, të analizojë dhe të marrë masa që të krijojë dhe zbatojë një skedulim të qartë dhe të dokumentuar për shqyrtimin e logeve të sistemit kritik e-Taxation të Drejtorisë së Përgjithshme të Tatimeve, ku të përcaktohet frekuenca e rishikimit dhe monitorimi, si dhe të krijohen procedura për trajtimin dhe dokumentimin e çdo incidenti të identifikuar gjatë procesit të monitorimit.

Brenda vitit 2025

11.1 Rekomandim: Agjencia Kombëtare e Shoqërisë së Informacionit, të marrë masa për të hartuar dhe zbatuar rregulla mbi menaxhimin e aksesit të palëve të treta në sistemet e Drejtorisë së Përgjithshme të Tatimeve dhe implementimin e mekanizmave të monitorimit dhe regjistrimit të veprimeve të tyre, për identifikimin e aktiviteteve të dyshimta ose të paautorizuara.

Menjëherë dhe në vijimësi

Për sa më sipër, paraqitet ky Raport Përfundimtar Auditimi.

KONTROLLI I LARTË I SHTETIT